

CYBER CRIME
MENURUT UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 11 TAHUN 2008 TENTANG ITE
(Perspektif Hukum Pidana Islam)



Tesis

Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh
Gelar Magister dalam Bidang Syariah/Hukum Islam
pada Program Pascasarjana UIN Alauddin
Makassar

Oleh:

Mohammad Haidar Ali

NIM: 80100208072

PROGRAM PASCASARJANA
UIN ALAUDDIN MAKASSAR
2012

PERNYATAAN KEASLIAN TESIS

Dengan penuh kesadaran, penulis yang bertanda tangan di bawah ini menyatakan bahwa tesis yang berjudul **“Cyber Crime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Perspektif Hukum Pidana Islam)”**, ini benar adalah hasil karya penulis sendiri. Jika di kemudian hari terbukti bahwa ia merupakan duplikat, tiruan, plagiat atau dibuat oleh orang lain secara keseluruhan atau sebagian, maka tesis dan gelar yang diperoleh karenanya batal demi hukum.

Makassar, 7 November 2012

Penulis,

Mohammad Haidar Ali

NIM: 80100208072

UNIVERSITAS ISLAM NEGERI
ALAUDDIN
M A K A S S A R

PENGESAHAN TESIS

Tesis dengan judul ***“Cyber Crime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Perspektif Hukum Pidana Islam)”*** yang disusun oleh **Mohammad Haidar Ali**, NIM: 80100208072, mahasiswa konsentrasi Syariah/Hukum Islam pada program Pascasarjana UIN Alauddin Makassar, telah diujikan dan dipertahankan dalam sidang *munaqasyah* yang diselenggarakan pada hari Selasa, 6 November 2012 M bertepatan dengan tanggal 21 Dzulhijjah 1433 H, dinyatakan telah dapat diterima sebagai salah satu syarat untuk memperoleh gelar Magister dalam bidang Syariah/Hukum Islam (dengan beberapa perbaikan).

PROMOTOR :

Prof. Dr. Sabri Samin, M.Ag. (.....)

KOPROMOTOR :

Dr. H. Abd. Rauf M. Amin, Lc., M.A. (.....)

PENGUJI :

1. Dr. Nur Taufik Sanusi, M.Ag. (.....)

2. Dr. H. Lomba Sultan, M.Ag. (.....)

3. Prof. Dr. Sabri Samin, M.Ag. (.....)

4. Dr. Abd. Rauf M. Amin, Lc., M.A. (.....)

Makassar, 7 November 2012 M
21 Dzulhijjah 1433 H

Ketua Program Studi
Dirasah Islamiyah,

Diketahui oleh:
Direktur Program Pascasarjana
UIN Alauddin Makassar,

Dr. Muljono Damopolii, M.Ag.
NIP: 19641110 199203 1 005

Prof. Dr. H. Moh. Natsir Mahmud, M.A.
NIP: 19540816 198303 1 004

KATA PENGANTAR

Puji dan syukur kehadiran Allah swt., karena atas izin-Nyalah, tesis yang berjudul *“Cyber Crime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Perspektif Hukum Pidana Islam)”* telah dapat diselesaikan dengan baik. Semoga penulisan tesis ini dapat bermanfaat bagi lembaga pendidikan secara umum. *Sfilawat* dan salam semoga selalu tercurahkan kepada Rasulullah saw., para keluarga, sahabat dan para pengikutnya yang selalu istikamah di jalan-Nya.

Dalam penulisan tesis ini, tidak sedikit hambatan dan kendala yang dialami, tetapi berkat usaha dan rasa optimis yang didorong oleh kerja keras yang tidak mengenal lelah, serta bantuan dari berbagai pihak, maka tesis ini dapat diselesaikan. Oleh sebab itu, kritik dan saran yang bersifat membangun dari semua pihak demi kesempurnaan penulisan tesis ini. Untuk itu, penulis menyampaikan penghargaan dan ucapan terima kasih terutama kepada:

1. Prof. Dr. H. A. Qadir Gassing HT, M.S., selaku Rektor UIN Alauddin Makassar, para Pembantu Rektor, dan seluruh Staf UIN Alauddin Makassar yang telah memberikan pelayanan maksimal.
2. Prof. Dr. H. Moh. Natsir Mahmud, M.A., selaku Direktur Program Pascasarjana (PPs) UIN Alauddin Makassar. Demikian pula kepada Prof. Dr. H. Baso Midong, M.Ag., dan Prof. Dr. H. Nasir A. Baki, M.A., selaku Asisten Direktur I dan II, dan

Dr. Muljono Damopolii, M.Ag., selaku Ketua Program Studi Dirasah Islamiyah pada Program Pascasarjana (PPs) UIN Alauddin Makassar.

3. Prof. Dr. Sabri Samin, M.Ag, selaku Ketua Konsentrasi Syariah/Hukum Islam pada Program Pascasarjana (PPs) UIN Alauddin Makassar.
4. Prof. Dr. Sabri Samin, M.Ag., dan Dr. H. Abd. Rauf M. Amin, Lc., M.A., selaku promotor dan kopromotor serta Dr. Nur Taufik Sanusi, M.Ag. dan Dr. H. Lomba Sultan, M.Ag. yang banyak meluangkan waktunya untuk memberikan bimbingan, petunjuk, koreksi, nasehat dan motivasi hingga terselesaikannya penulisan tesis ini.
5. Para Dosen Pascasarjana UIN Alauddin Makassar dengan segala jerih payah dan ketulusan, bimbingan dan memandu perkuliahan sehingga memperoleh wawasan dan keilmuan yang luas.
6. Seluruh Karyawan dan Staf Tata Usaha PPs UIN Alauddin Makassar yang telah banyak membantu kami dalam pengurusan dan penyelesaian segala administrasi.
7. Kepala Perpustakaan Pusat UIN Alauddin Makassar beserta segenap stafnya yang telah menyiapkan literatur dan memberikan kemudahan untuk dapat memanfaatkan secara maksimal demi penyelesaian tesis ini.
8. Kedua orang tua, Ayahanda H. Alit Sukardi AM dan Ibunda (almh) Hj. Musri'ah yang telah mengasuh, mendidik, dan membimbing sejak kecil sampai dewasa yang disertai dengan doa.

9. Seluruh keluarga yang telah mendoakan dan membantu baik secara moral maupun material, sehingga penulis dapat menyelesaikan studi di Program Pascasarjana.
10. Rekan-rekan mahasiswa Program Pascasarjana UIN Alauddin Makassar, sahabat, dan teman-teman yang telah memberikan bantuan, motivasi, kritik, saran, dan kerjasama selama perkuliahan dan penyusunan tesis ini.
11. Kepada semua pihak yang tidak sempat disebutkan satu persatu, yang telah membantu serta menyumbangkan pemikiran kepada penulis.

Akhirnya, semoga hasil penulisan tesis ini dapat bermanfaat dan semoga pula segala partisipasi semua pihak akan memperoleh imbalan yang berlipat ganda dari Allah swt. Amin.

Makassar, 7 November 2012

Penulis,

Mohammad Haidar Ali

NIM: 80100208072

UNIVERSITAS ISLAM NEGERI
ALAUDDIN
M A K A S S A R

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
PERNYATAAN KEASLIAN TESIS	ii
PENGESAHAN TESIS	iii
KATA PENGANTAR	iv
DAFTAR ISI	vii
DAFTAR TRANSLITERASI.....	ix
ABSTRAK.....	xii
 BAB I PENDAHULUAN.....	 1-30
A. Latar Belakang Masalah	1
B. Rumusan dan Batasan Masalah	12
C. Definisi Operasional dan Ruang Lingkup Penelitian	13
D. Kajian Pustaka	16
E. Kerangka Teoretis	19
F. Metodologi Penelitian	24
G. Tujuan dan Kegunaan Penelitian	27
H. Garis Besar Isi Tesis	29
 BAB II TINJAUAN UMUM <i>CYBER CRIME</i>	 31-56
A. Pengertian <i>Cyber Crime</i>	31
B. Jenis-Jenis <i>Cyber Crime</i>	37
C. Sejarah <i>Cyber Crime</i>	51
D. Ruang Lingkup <i>Cyber Crime</i>	54
 BAB III KONSEPSI <i>CYBER CRIME</i> DALAM HUKUM PIDANA DI INDONESIA	 57-136
A. Hakikat <i>Cyber Crime</i> dan Eksistensinya dalam Undang-Undang ITE.....	57
B. Faktor-faktor yang Memengaruhi Terjadinya <i>Cyber Crime</i>	63
C. Modus Operandi Terjadinya <i>Cyber Crime</i>	78
D. Penanggulangan <i>Cyber Crime</i> Berdasarkan Perundang-undangan di Indonesia	81
E. Unsur-unsur Tindak Pidana dalam <i>Cyber Crime</i>	88
F. Pembuktian <i>Cyber Crime</i> dalam Hukum Pidana di Indonesia.....	95

G. Sanksi Pidana Bagi Pelaku <i>Cyber Crime</i>	125
BAB IV MENCARI AKAR <i>CYBER CRIME</i> DALAM ISLAM.....	137-253
A. Perspektif Hukum Pidana Islam tentang <i>Cyber Crime</i>	137
B. <i>Cyber Crime</i> dan Relevansinya dengan Jarimah	143
C. <i>Cyber Crime</i> dan Korelasinya dalam Pembagian Hukum Pidana Islam	151
D. Pembuktian <i>Cyber Crime</i> dalam Hukum Pidana Islam	164
E. Sanksi Pidana <i>Cyber Crime</i> dalam Hukum Pidana Islam	192
BAB VI PENUTUP	203-201
A. Kesimpulan	203
B. Rekomendasi Penelitian	205
DAFTAR PUSTAKA	207-214
LAMPIRAN-LAMPIRAN:	215-253
1. Daftar Jenis Pidana dan Sanksi Pidana Kejahatan <i>Cyber Crime</i> Menurut Undang-Undang RI Nomor 11 Tahun 2008 tentang ITE	215
2. Undang-Undang RI Nomor 11 Tahun 2008 tentang ITE	218
3. Penjelasan atas Undang-Undang RI Nomor 11 Tahun 2008 tentang ITE	240
DAFTAR RIWAYAT HIDUP	254-255

UNIVERSITAS ISLAM NEGERI
ALAUDDIN
M A K A S S A R

TRANSLITERASI DAN SINGKATAN

A. Transliterasi

1. Konsonan

Huruf-huruf bahasa Arab ditransliterasi ke dalam huruf latin sebagai berikut :

= -	= z	= q
= B	= s	= k
= T	= sy	= l
= s	= s}	= m
= J	= d}	= n
= h}	= t}	= w
= kh	= z}	ه = h
= D	= ‘	= ‘
= z	= g	= y
= R	= f	

Hamzah () yang terletak di awal kata mengikuti vokalnya tanpa diberi tanda apa pun. Jika ia terletak di tengah atau di akhir, maka ditulis dengan tanda (’).

4. Vokal

Vokal (a) panjang	= a>	: <i>matā</i>
Vokal (i) panjang	= i>	قِيلَ : <i>qīla</i>
Vokal (u) panjang	= u>	يَمُوتُ : <i>yamutu</i>

5. Diftong

= aw	هَوْلَ : <i>hauḷa</i>
= ay	كَيْفَ : <i>kaifa</i>

6. Kata Sandang

() alif lam ma'rifah ditulis dengan huruf kecil jika terletak ditengah kalimat dan besar bila di awal kalimat, contoh:

- a. Hadis riwayat al-Bukhari>
- b. Al-Bukhari>meriwayatkan

7. *Ta' marbutah*

Ta' marbutah ditransliterasi dengan (t) jika terletak ditengah kalimat, tetapi jika terletak di akhir kalimat maka ditransliterasikan dengan huruf (h).

8. *Lafz} al-Jalalah* ()

Kata “Allah” yang didahului partikel seperti huruf *jarr* dan huruf lainnya atau berkedudukan sebagai *mudhaf* ilaih (frasa nominal), ditransliterasi tanpa huruf hamzah. Contoh: *دِينُ اللَّهِ* *diṭullāh* *billāh*

Adapun *ta marbutah* di akhir kata yang disandarkan kepada *lafz} al-jalalah*, ditransliterasi dengan huruf [t]. Contoh: *هُم فِي رَحْمَتِ اللَّهِ* *hum fi rahmatillah*

9. *Tasydid*

Tasydid ditambah dengan konsonan ganda kata-kata atau istilah Arab yang sudah menjadi bagian dari perbendaharaan bahasa Indonesia, tidak ditulis lagi menurut cara transliterasi ini.

10. Singkatan

- swt. = *subḥānuhū wa ta'ālā*
saw. = *ṣallallāhu 'alaihi wa sallam*
a.s. = *'alaihi al-salam*
H = Hijrah
M = Masehi

SM = Sebelum Masehi

l. = Lahir tahun (untuk orang yang masih hidup saja)

w. = Wafat tahun



ABSTRAK

Nama : Mohammad Haidar Ali

NIM : 80100208072

Judul Tesis : **“Cyber Crime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang ITE (Perspektif Hukum Pidana Islam)”**

Tesis ini membahas tentang *cyber crime* menurut Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik perspektif hukum pidana Islam. Adapun masalah yang dikemukakan dalam tesis ini adalah sebagai berikut; *Pertama*, bagaimana hakikat *cyber crime* dan eksistensinya dalam Undang-Undang ITE? *Kedua*, bagaimana perspektif hukum pidana Islam tentang *cyber crime*? *Ketiga*, bagaimana bentuk sanksi pidana *cyber crime* menurut hukum pidana di Indonesia dan hukum pidana Islam? Adapun tujuan dari penelitian ini adalah untuk mengetahui hakikat *cyber crime* dan eksistensinya dalam Undang-Undang ITE, untuk mengetahui *cyber crime* menurut perspektif hukum pidana Islam, dan untuk mengetahui bentuk sanksi pidana *cyber crime* menurut hukum pidana di Indonesia dan hukum pidana Islam.

Untuk mengurai lebih jauh pokok permasalahan dalam tesis ini, mengacu pada pendekatan *multidisipliner* yaitu pendekatan teologis normatif (*syar'i*), yuridis normatif, sosiologis dan historis. Penelitian ini tergolong *library research* yang dikumpulkan dari buku-buku dan literatur yang berhubungan dengan pembahasan. Selanjutnya data yang diperoleh diinventarisir diseleksi sesuai dengan masalah tersebut dan dikaji serta dianalisis dengan metode kualitatif eksplanatif dan dengan *content analysis* (analisis isi).

Hasil dari penelitian ini mengungkapkan beberapa hal yaitu; *pertama*, *cyber crime* dalam Undang-Undang ITE pada hakikatnya adalah kejahatan yang dilakukan oleh pelaku dengan menggunakan sarana teknologi informasi (internet) dan sejenisnya. Perbuatan *cyber crime* telah diatur secara spesifik melalui Undang-Undang ITE tercantum dalam Bab 7 untuk “Perbuatan yang Dilarang” yakni pada Pasal 27-37 dan dalam Bab 11 untuk “Ketentuan Pidana” pada Pasal 45-52. *Kedua*, hukum pidana Islam melihat *cyber crime* sebagai suatu kejahatan nyata, tetapi maya yang mengalami modernisasi pada aspek modus operandi dan memiliki kesamaan terhadap hukum pidana Islam pada aspek substansi. Karena kejahatan yang terjadi pada dunia *cyber* merupakan pengembangan dari bentuk kejahatan yang cikal

bakalnya telah ada pada zaman dahulu kala dan berkembang secara pesat melalui perkembangan teknologi informasi. Kejahatan yang terlihat pada saat ini merupakan bentuk modernisasi yang mengiringi perkembangan *cyber cpace* (dunia maya/internet). *Cyber crime* dilihat dari sudut pandang hukum pidana Islam yang menjadi landasan pokok terhadap aspek yuridis, adalah teori *maqasid al-syari'ah* meletakkan prinsip-prinsip yang menjadi pertimbangan pokok dari tujuan hukum, yaitu terwujudnya kemaslahatan manusia baik di dunia maupun di akhirat, yaitu terwujud dan terpeliharanya *al-masā'il al-khamsah* atau lima kebutuhan pokok dalam kehidupan manusia yang mencakup pemeliharaan agama (*hifz al-din*), jiwa (*hifz al-nafs*), keturunan atau kehormatan (*hifz al-nasl*), harta (*hifz al-māl*) dan akal (*hifz al-'aql*). Sehingga kenyataan dalam praktik-praktik *cyber crime* dinilai melanggar lima kebutuhan pokok dalam kehidupan manusia tersebut. Ketiga, adapun sanksi pidana bagi penipuan, kesusilaan, perjudian, pengancaman, perusakan, dan pencurian dapat dilihat dalam Undang-Undang ITE. Sedangkan dalam hukum pidana Islam, sanksi pidana ditentukan berdasarkan *jarimah hudud*, *jarimah qisas* dan diat, dan *jarimah ta'zir*.

Rekomendasi dari penelitian ini adalah, bahwa reregulasi dan optimalisasi esensi hukum dan perundang-undangan di Indonesia diperlukan untuk mewujudkan *law an forcement* dan kepastian hukum. Hal ini didasarkan oleh lahirnya banyak perundang-undangan yang kurang menyentuh substansi hukum, yakni terciptanya rasa keadilan, keamanan dan ketentraman masyarakat.

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Hukum pidana di Indonesia menurut catatan sejarah mengalami perubahan yang sangat signifikan, karena sejalan dengan perkembangan sosial budaya masyarakat di mana hukum tersebut diberlakukan. Dalam kaitan itu, hukum selalu berubah-ubah karena kejahatan yang terjadi juga berubah-ubah dan cenderung mengalami perkembangan.

Untuk menjawab problem tersebut dibutuhkan perangkat hukum yang memadai, sehingga penegakan hukum (*law enforcement*) tidak mengalami kesulitan dalam melakukan proses penegakannya. Selama ini aparaturnya penegak hukum mengalami kesulitan dikarenakan terjadi kekosongan hukum¹ yang disebabkan adanya kejahatan-kejahatan baru yang belum terakomodir dalam undang-undang. Sejalan dengan hal tersebut, kejahatan yang bersifat tradisional terus berkembang seiring dengan perubahan zaman yang terus maju.

Peradaban manusia mengalami perubahan drastis dalam dekade pada penghujung Abad ke-19. Perubahan tersebut terutama menyangkut interaksi dan pergaulan yang tidak terbatas dengan menggunakan media telekomunikasi. Dalam tata pergaulan dunia yang baru itu, tidak terlihat lagi sekat-sekat atau batas suatu negara. Tidak lagi dipersoalkan warna kulit, ras dan golongan. Karena tidak lagi

¹Kekosongan hukum terjadi disebabkan adanya perkembangan dunia modern, seperti terciptanya pembangkit listrik, internet dan sarana telekomunikasi yang lainnya. Dari perkembangan tersebut, hukum belum menjangkau terhadap perkembangannya. Oleh karena itu, diperlukan daya jangkau hukum yang universal untuk mengikuti perkembangannya.

mengindahkan jarak dan waktu, hubungan dapat dilakukan kapan saja, di mana saja dan dari mana saja. Hal inilah yang dikenal sebagai hubungan global.²

Indonesia merupakan bagian dari tata pergaulan hubungan global tersebut. Sebagai masyarakat global, manusia harus melaksanakan pemahaman dunia dalam tatanan yang baru, sehingga dalam mewujudkan negara yang maju harus mampu menempatkan dan memosisikan diri sebagai negara yang siap dan mampu dalam menghadapi persaingan global.

Perkembangan teknologi khususnya di bidang telekomunikasi dianggap sebagai lokomotif dan turut mempercepat proses globalisasi pada berbagai aspek kehidupan.³ Perusahaan telekomunikasi seperti *microsoft word* memberikan berbagai fasilitas dan kemudahan dalam mengakses aneka kebutuhan informasi atas dukungan *soft ware* dan *hard ware* yang dihasilkan. Kebutuhan atas peningkatan arus informasi antar manusia, dengan kemampuan mengirim dan menerima data dan informasi melalui jaringan komputer menjadi kebutuhan yang tidak dapat dipungkiri.⁴

Teknologi informasi (*information technology*) memegang peran penting, baik pada masa kini maupun masa yang akan datang. Teknologi informasi diyakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia. Ada 2 (dua) hal yang menjadikan teknologi informasi dianggap penting dalam memacu pertumbuhan ekonomi dunia. *Pertama*, teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu, seperti komputer, modem, sarana untuk

²Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya* (Cet. I; Yogyakarta: Laksbang Pressindo, 2007), h. 1.

³Muhammad Aulia Adnan, *Tinjauan Hukum dalam E-Business* Olyx76@yahoo.com. (Diakses pada tanggal, 25 Juni 2010)

⁴Sutarman, *op. cit.*, h. 2.

membangun jaringan internet dan sebagainya. *Kedua*, memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya.⁵

Kemajuan teknologi informasi sekarang dan pada masa yang akan datang tidak lepas dari dorongan yang dilakukan oleh perkembangan teknologi komunikasi dan teknologi komputer, sedangkan teknologi komputer dan telekomunikasi didorong oleh teknologi mikro elektronika, material dan perangkat lunak.

Kemajuan teknologi telah mengubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Pada perkembangan teknologi informasi tersebut berpadu dengan media dan komputer. Lahirlah piranti baru yang dinamakan internet. Kehadiran internet ini telah mengubah paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (*real*) bertambah dengan realitas baru yang bersifat maya (*virtual*). Realitas yang kedua ini sering dikaitkan dengan internet dan *cyber space*.⁶

Di samping itu, perubahan paradigma ini juga diikuti perubahan cara pandang baru. Cara pandang baru yang dimaksud adalah dokumentasi yang semula *paper based* menjadi *elektronik based*. Hal ini menjadi sangat jelas ketika melakukan transaksi lewat pasar *on-line* (internet). Dalam transaksi ini akan terlihat bahwa keseluruhannya serba berbasis elektronik, misalnya *digital signature*, *e-mail*.⁷

⁵Agus Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Cet. I; Bandung: PT Citra Aditya Bakti, 2002), h. 1.

⁶Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Cet. I; Bandung: Refika Aditama, 2005), h. 103.

⁷*Ibid.*, h. 104.

Teknologi informasi (*information technology*) membawa dampak bagi masyarakat secara luas, baik dampak positif maupun negatif. Dampak positifnya adalah dapat memperoleh berbagai informasi, baik dari dalam maupun luar negeri, transaksi jarak jauh. Sedangkan dampak negatifnya adalah memberikan peluang untuk melakukan berbagai kejahatan, seperti penipuan, pencurian, pencemaran nama baik, kesusilaan, perjudian, pengancaman, perusakan dan teror yang seluruhnya dikenal dengan *cyber crime*.

Cyber crime adalah kejahatan yang dilakukan oleh seseorang, sekelompok orang dan korporasi (badan hukum) dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer. Kejahatan ini terjadi di dunia maya (*virtual*) sehingga mempunyai karakteristik yang berbeda dengan kejahatan tradisional.⁸ Berdasarkan beberapa hasil penelitian, karakteristik pelaku *cyber crime* sangat unik, dan juga berbeda kategori dengan pelaku kejahatan lain. Saat ini, meskipun hukum pidana konvensional sebagaimana yang berlaku di Indonesia dapat digunakan hakim sebagai dasar hukum untuk mengadili pelaku *cyber crime*, akan tetapi dalam praktik sangat banyak keterbatasannya, baik dari sisi unsur tindak pidana maupun pertanggungjawaban pidananya. Akibatnya, banyak pelaku yang lolos dari jeratan hukum. Berdasarkan hasil penelitian yang dilakukan oleh Widodo dalam "*Sistem Pemidanaan dalam Cyber Crime*" semua pelaku dijatuhi pidana penjara. Dalam tataran filosofis, teoretis, normatif maupun empiris, pidana

⁸Kejahatan tradisional adalah kejahatan yang dilakukan tanpa menggunakan sarana internet, telekomunikasi atau sarana canggih.

penjara merupakan suatu jenis pidana yang mempunyai banyak kelemahan karena pelaksanaan pidana penjara khususnya di Indonesia kurang memadai.⁹

Menurut Widodo, penjatuan pidana penjara para pelaku *cyber crime* adalah langkah yang kurang bijak. Hal ini disebabkan oleh ketidaksesuaian antara karakteristik pelaku tindak pidana dengan sistim pembinaan narapidana di Lembaga Pemasyarakatan, sehingga tujuan pemidanaan sebagaimana diatur dalam Undang-Undang Pemasyarakatan tidak akan tercapai. Menurut Widodo, sebagai pengganti pemidanaan tersebut adalah pidana kerja sosial atau pidana pengawasan,¹⁰ karena ada kesesuaian antara karakteristik pelaku *cyber crime* dengan paradigma pemidanaan dalam pidana kerja sosial atau pidana pengawasan, sehingga tujuan pemidanaan dapat dicapai.¹¹

Sejalan dengan pandangan Widodo, dalam mengantisipasi *cyber crime*, Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana (RUU KUHP)¹² mencoba memperluas cakupan istilah untuk dapat membidik dan menjaring kejahatan tersebut.

Sedangkan menurut Barda Nawawi Arief, dilihat dalam perspektif hukum pidana, upaya penanggulangan *cyber crime* dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggung-

⁹Widodo, *Sistem Pemidanaan dalam Cyber Crime: Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime* (Cet. I; Yogyakarta: Laksbang Mediatama, 2009), h. iii.

¹⁰Pidana kerja sosial dan pidana pengawasan termasuk jenis-jenis pemidanaan yang tercantum dalam RUU KUHP Tahun 2007 pada Pasal 65 ayat 1.

¹¹Widodo, *op. cit.*, h. vi.

¹²Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana (RUU KUHP) selanjutnya disebut RUU KUHP.

jawaban pidana atau pemidanaan (termasuk aspek pembuktian dan alat bukti), dan aspek yurisdiksi.¹³

Berkaitan dengan hal tersebut, perumusan tindak pidana di dalam KUHP masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cyber crime*. Di samping itu, mengandung berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan *hitech crime* (kejahatan berteknologi tinggi) yang sangat bervariasi. Misalnya, untuk menghadapi masalah pemalsuan kartu kredit dan transfer dana elektronik, dalam KUHP tidak ada ketentuan khusus mengenai pembuatan kartu kredit, yang ada hanya ketentuan mengenai; sumpah/keterangan palsu tercantum pada Bab IX Pasal 242 KUHP, pemalsuan mata uang dan uang kertas pada Bab X Pasal 244-252 KUHP, tentang pemalsuan pada Bab XI Pasal 253-262 KUHP, pemalsuan surat pada Bab XII Pasal 263-276 KUHP.¹⁴

Kemungkinan dalam praktik digunakan pasal-pasal lain yang berkaitan dengan penggunaan kartu kredit palsu (untuk melakukan kejahatan), bukan pembuatannya. Hal inilah yang ingin dilihat, bahwa dalam KUHP belum sepenuhnya mampu menjaring kejahatan tersebut, melainkan memunculkan potensi terlepasnya kejahatan-kejahatan tersebut dari jeratan hukum. Dengan demikian diperlukan perangkat hukum yang mampu menunjangnya. Untuk itu, diperlukan menarik undang-undang yang dinilai sudah tidak relevan dengan perkembangan zaman kepada undang-undang yang *up to date* yang mampu menjawab perkembangan zaman.

¹³Lihat Barda Nawawi Arief, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan* (Cet. I; Bandung: PT Citra Aditya Bakti, 2005), h. 125.

¹⁴*Ibid.*, h. 127-128.

Berkaitan dengan hal tersebut, Indonesia mencoba melakukan kebijakan harmonisasi dengan negara-negara lain, khususnya dalam lingkungan Asia dan Asean menyangkut masalah *cyber crime*. Antisipasi masalah *cyber crime* tidak hanya melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun juga berusaha mengantisipasinya dalam penyusunan RUU KUHP. Kebijakan yang ditempuh dalam konsep RUU KUHP tahun 2002 memperluas dan memberikan penjelasan definisi tentang beberapa aspek yang secara langsung maupun tidak langsung berkaitan dengan masalah *cyber crime*.¹⁵

Dalam Buku I RUU KUHP Indonesia pada Pasal 174 dalam Ketentuan Umum, disebutkan tentang pengertian “barang”, yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon, telekomunikasi, atau jasa komputer. Adapun redaksi teks Pasal 174 sebagai berikut:

Barang adalah benda berwujud termasuk air dan uang giral, dan benda tidak berwujud termasuk aliran listrik, gas, data dan program komputer, jasa telepon, jasa telekomunikasi, atau jasa komputer.¹⁶

Pengertian tersebut secara tegas mengakui bahwa benda atau barang tidak berwujud merupakan barang atau benda yang dapat dijadikan alat bukti.¹⁷

Dalam Buku I RUU KUHP Indonesia Pasal 188 juga dicantumkan tentang pengertian “surat”, mencakup data tertulis atau tersimpan dalam disket, pita

¹⁵Lihat Teguh Arifiyadi dalam <http://webcache.googleusercontent.com/search?q=cache:dO6u5UYvFAMJ:blogs.depkominfo.go.id/itjen/2008//12/19/cyber-crime-dalam-perspektif-rancangan-konsep-kuhp-baru/+cyber+crime&cd=10&hl=id&ct=clnk&gl=id>. (Diakses pada tanggal, 25 Juni 2010)

¹⁶Barda Nawawi Arief, *op. cit.*, h. 131.

¹⁷Barang berwujud adalah barang yang tampak oleh panca indra penglihatan manusia tanpa melalui jaringan internet atau komputer, seperti *paper based*. Sedangkan barang tidak berwujud adalah barang yang secara kasat mata tampak melalui jaringan internet atau komputer, seperti *electronic based*, *software* dan lain-lain.

magnetik, media penyimpan komputer atau penyimpan data elektronik lainnya.

Dalam pasal tersebut dinyatakan:

Surat adalah selain surat yang tertulis di atas kertas, juga surat atau data yang tertulis atau tersimpan dalam disket, pita magnetik, atau media penyimpan komputer atau media penyimpan data elektronik lain.¹⁸

Definisi “surat” menggambarkan makna surat secara berwujud (tertulis) dan tidak berwujud (*virtual*). Makna surat yang tidak berwujud dapat berupa *e-mail*, *massage* dalam *chatting/guest book situs*, komentar tertulis dalam sebuah situs/*file* dalam bentuk aplikasi apapun, *short message service* (SMS) atau *blackberry massager* (BBM), termasuk di dalamnya *software* (perangkat lunak).

Berdasarkan 2 (dua) pasal tersebut, dapat menjadi gambaran untuk melihat *cyber crime* dari sudut pandang RUU KUHP. Hal ini dimaksudkan untuk mencegah dan mengurangi kejahatan yang terjadi dalam dunia maya. Selain itu, agar pelaku kejahatan yang berkaitan dengan kemajuan berteknologi dapat dijerat dengan undang-undang tersebut.

Dilihat dari aspek pokok aktivitasnya, *cyber crime* dilakukan lebih menitik-beratkan pada penyerangan *content*, *computer system* dan *communication system* milik orang lain, baik secara personal maupun umum di dalam *cyber space*.¹⁹ Untuk itu, diperlukan pengamanan sebuah sistem untuk mencegah terjadinya kerusakan.

Pada aspek lain, penanggulangan *cyber crime* dilakukan dengan pencegahan dan penegakan hukum, demi tercapainya supremasi hukum. Apabila dibiarkan terus

¹⁸*Ibid.*

¹⁹http://www.lintasberita.com/teknologi/pengertian_cyber_crime. (Diakses pada tanggal, 1 Juni 2011). *Cyber space* (ruang maya) adalah terhubungnya komputer dengan saluran penyedia jasa internet yang dapat diakses kapan saja, tidak mengenal batas ruang dan waktu. Akses dapat dilakukan untuk transaksi jual beli barang, tukar informasi, mencari informasi atau bahkan merusak suatu jaringan komputer yang digelar oleh siapapun, baik pemerintah maupun swasta.

menerus, dapat mengganggu keamanan baik secara nasional maupun internasional. Sesungguhnya *cyber crime* sudah mengganggu keamanan dalam negeri maupun luar negeri, sehingga diperlukan langkah-langkah strategis aparat penegak hukum untuk menanggulangnya.

Cyber crime secara substansial tidak jauh berbeda dengan hukum pidana Islam baik secara karakteristiknya maupun unsur-unsurnya. Misalnya pencurian, unsur-unsur yang terkandung dalam pencurian dimiliki oleh keduanya seperti, mengambil barang yang bukan haknya, mengambil tanpa sepengetahuan pemiliknya, ingin memiliki terhadap barang tersebut dan unsur-unsur yang lainnya. Secara karakteristik keduanya juga memiliki kesamaan, yakni adanya fakta peristiwa hukum yang terjadi. Hanya saja dalam *cyber crime* terjadi secara *virtual* (maya).²⁰

Selain itu, *cyber crime* terjadi karena kontrol personal dan kontrol sosial lemah. Hal ini disebabkan karena kejahatan ini bersifat maya (*virtual*), ketika pelaku tidak tampak secara fisik. Dalam pendekatan normatif, *cyber crime* ini ada yang merupakan kejahatan konvensional tetapi dengan modus baru seperti, pornografi, penipuan, pencemaran nama baik dan sebagainya, yang menggunakan media internet sebagai sarana untuk melakukan kejahatan, maka dapat dipidana dengan melihat Kitab Undang-Undang Hukum Pidana (KUHP), sementara itu terhadap *cyber crime* jenis baru seperti *hacking*, kejahatan ini tidak ada ketentuan dalam KUHP. Dengan demikian terjadi kekosongan hukum (*rechts vacuum*).²¹

²⁰*Cyber crime* bersifat nyata (*real*) tetapi maya (*virtual*) adalah kenyataan suatu peristiwa hukum yang terjadi dalam ruang maya (*cyber space*) atau internet. Secara yuridis aktivitas tersebut tidak dapat dideteksi dengan ukuran dan kualifikasi hukum konvensional, karena apabila cara ini yang ditempuh akan banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Oleh karena itu, hal ini perlu dilengkapi fasilitas aturan hukum yang serupa dan sepadan. Seperti halnya Undang-Undang RI No. 11 Tahun 2008 tentang ITE yang mencoba menjangkau ruang maya tersebut.

²¹Nia Kurnia dalam http://student-research.umm.ac.id/index.php/departement_of_syariah/

Lahirnya Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)²² telah dinilai mampu mengakomodir jenis kejahatan yang merupakan pengembangan terhadap kejahatan melalui media internet. Selain itu, undang-undang tersebut diharapkan menjadi jawaban konkrit terhadap problem yang dihadapi oleh aparaturnya penegak hukum.

Dalam perspektif hukum pidana Islam, *cyber crime* termasuk tindakan perusakan terhadap tatanan nilai-nilai sosial dalam dunia teknologi informasi yang berdampak terhadap struktur masyarakat luas baik secara nasional maupun internasional. Dampak tersebut dapat dirasakan ketika lalu lintas di dunia *space* penggunaanya menjadi korban, baik secara finansial maupun sosial khususnya maraknya pencurian lewat pasar *on line* dan mania *facebook*s yang berdampak pada korban gadis di bawah umur menghilang tanpa diketahui oleh keluarganya.²³

Dengan demikian *cyber crime* adalah tindakan yang dilarang oleh Allah swt., karena Allah swt. tidak menyukai orang-orang yang membuat kerusakan yang memudharatkan orang lain. Perusakan dalam bentuk apapun tidak dibenarkan, karena perusakan merupakan tindakan yang bertentangan dengan nilai-nilai universal. Allah swt. secara tegas berfirman dalam Q.S. Al-Maidah/5: 64 sebagai berikut:

وَقَالَتِ الْيَهُودُ يَدُ اللَّهِ مَغْلُولَةٌ غُلَّتْ أَيْدِيهِمْ وَلَعْنُوا بِمَا قَالُوا ۚ بَلْ يَدَاهُ مَبْسُوطَتَانِ يُنفِقُ كَيْفَ يَشَاءُ ۚ وَلَيَزِيدَنَّ كَثِيرًا مِّنْهُمْ مَا أُنْزِلَ إِلَيْكَ مِنْ رَبِّكَ طُغْيَانًا وَكُفْرًا ۚ وَأَلْقَيْنَا بَيْنَهُمُ

article/view/7253/0 (diakses pada tanggal, 5 Oktober 2012).

²²Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) selanjutnya disebut Undang-Undang ITE.

²³Kasus menghilangnya gadis di bawah umur berdasarkan laporan dari media tidak sekedar anak tersebut menjadi korban penculikan, tetapi juga menjadi korban pelecehan seksual sekaligus berakhir dari kematian.

الْعَدَاوَةَ وَالْبَغْضَاءَ إِلَى يَوْمِ الْقِيَامَةِ ۚ كُلَّمَا أَوْقَدُوا نَارًا لِلْحَرْبِ أَطْفَأَهَا اللَّهُ ۚ وَيَسْعَوْنَ فِي الْأَرْضِ فَسَادًا ۚ وَاللَّهُ لَا يُحِبُّ الْمُفْسِدِينَ

Terjemahnya:

Dan orang-orang Yahudi berkata: “Tangan Allah terbelenggu”. Sebenarnya tangan merekalah yang dibelenggu dan merekalah yang dilaknat disebabkan apa yang telah mereka katakan itu. Padahal kedua tangan Allah terbuka; Dia memberi rezki sebagaimana dia kehendaki. Dan (Alquran) yang diturunkan kepadamu dari Tuhanmu itu pasti akan menambah kedurhakaan dan kekafiran bagi kebanyakan mereka. Dan Kami timbulkan permusuhan dan kebencian di antara mereka sampai hari kiamat. Setiap mereka menyalakan api peperangan, Allah memadamkannya dan mereka berbuat kerusakan dimuka bumi dan Allah tidak menyukai orang-orang yang membuat kerusakan.²⁴

Ayat tersebut menegaskan bahwa tindakan perusakan merupakan sesuatu yang dilarang oleh Allah swt. baik dalam bentuk apapun dan di manapun, tetap tidak dibenarkan. Tindakan para *hacker*²⁵ menjadi bagian dari perbuatan dan tindakan yang sangat dominan dilakukan oleh para pelaku kejahatan *cyber crime* yang dilarang sebagaimana ayat tersebut. Landasan larangan tersebut mengarah kepada hal-hal yang merugikan dan meresahkan orang lain.

Dalam hukum pidana Islam, kejahatan dunia maya (*cyber crime*) merupakan bagian jarimah takzir. Jarimah takzir adalah jarimah dan hukuman yang belum ditetapkan oleh syarak dan wewenang untuk menetapkan diserahkan kepada *ulil amri* (pemerintah/hakim), dengan pertimbangan hukuman itu dapat mencegah

²⁴Departemen Agama RI, *Alquran dan Terjemahnya* (Cet. X; Bandung: PT. Syamil Cipta Media, 2006), h. 118.

²⁵*Hacker* adalah orang yang memasuki atau mengakses sistem jaringan komputer secara tidak sah (tanpa izin) dengan suatu alat dan program tertentu bertujuan untuk merusak, mengubah data dengan menambah atau mengurangi. Kejahatan yang dilakukan *hacker* berdampak terhadap kerusakan jaringan komputer.

pelakunya untuk tidak mengulangnya kembali dan hukumannya disesuaikan dengan tingkat kejahatan.²⁶

Berdasarkan metode yang digunakan, maka diketahui bahwa sanksi kejahatan *carding* menurut Undang-Undang ITE terdapat dalam Pasal 30 dan 31 yang intinya mengakses sistem elektronik orang lain tanpa sepengetahuan pemiliknya. Sedangkan dalam hukum pidana Islam sanksi kejahatan *carding* dilihat menggunakan metode kias, karena alat hukumnya serupa dengan pencurian. Dalam undang-undang konvensional yang dinilai tidak cukup memadai untuk menjawab problematika *cyber crime*, maka Undang-Undang ITE diharapkan menjadi jawaban yang tepat sasaran. Akan tetapi, bagaimana undang-undang tersebut menurut perspektif hukum pidana Islam?

Oleh karena itu, menarik untuk diteliti Undang-Undang ITE terkait dengan pasal-pasal yang mengandung tindak pidana mayantara (*cyber crime*) berdasarkan hukum pidana Islam terutama terkait dengan pembuktian di depan sidang pengadilan.

B. Rumusan dan Batasan Masalah

1. Rumusan Masalah

Berdasarkan latar belakang masalah tersebut, maka yang menjadi permasalahan pokok dalam penulisan ini adalah bagaimana *cyber crime* menurut Undang-Undang ITE perspektif hukum pidana Islam?

Berdasarkan masalah pokok tersebut, maka dapat dikemukakan sub masalah yaitu:

²⁶Nia Kurnia, *op. cit.*

- a. Bagaimana hakikat *cyber crime* dan eksistensinya dalam Undang-Undang ITE?
- b. Bagaimana perspektif hukum pidana Islam tentang *cyber crime* ?
- c. Bagaimana bentuk sanksi pidana *cyber crime* menurut hukum pidana di Indonesia dan hukum pidana Islam?

2. Batasan Masalah

Berdasarkan rumusan masalah tersebut, maka batasan masalahnya adalah Undang-Undang ITE yang berkaitan dengan tindak pidana penipuan, kesusilaan, perjudian, pengancaman, perusakan dan penipuan. Batasan masalah ini perlu dihadirkan, untuk mempermudah objek kajian dalam tesis ini, sehingga kajiannya tidak keluar dari pokok yang telah dirumuskan.

C. Definisi Operasional dan Ruang Lingkup Penelitian

1. Definisi Operasional

Untuk menghindari terjadinya penafsiran yang keliru terhadap judul tesis ini, perlu dijelaskan pengertian dari beberapa istilah/variabel.

a. *Cyber Crime*

Menurut Kamus Bahasa Inggris-Indonesia *cyber* berarti maya, sedangkan *crime* adalah *an offence which is punishable by law* (suatu kejahatan yang dihukum oleh hukum), *illegal activity in general* (kegiatan ilegal pada umumnya), atau *a bad, immoral, or dishonourable act* (tidak terhormat, tidak bermoral, atau tindakan yang buruk).²⁷ Menurut Kamus Bahasa Inggris-Indonesia *crime* diartikan dengan

²⁷Longman Group, *Longman dictionary of Contemporary English* (Ed. VIII; England: [t.tp], 1998), h. 155.

kejahatan.²⁸ Secara kebahasaan *cyber crime* samakna dengan “kejahatan dunia maya” atau “kejahatan mayantara”.²⁹

Cyber crime dalam tesis ini adalah kejahatan yang dilakukan oleh seseorang, kelompok maupun korporasi dengan menggunakan sarana komputer dan alat telekomunikasi lainnya seperti *hand phone* sebagai dampak negatif dari perkembangan aplikasi internet.

b. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

Secara etimologi, undang-undang mengandung beberapa arti, yakni:

1. Ketentuan dan peraturan negara yang dibuat oleh pemerintah (menteri, badan eksekutif, dan sebagainya), disahkan oleh parlemen (Dewan Perwakilan Rakyat, badan legeslatif, dan sebagainya), ditandai tangani oleh kepala negara (presiden, kepala pemerintah, raja), dan mempunyai kekuatan yang mengikat;
2. Aturan yang dibuat oleh orang atau badan yang berkuasa;
3. Hukum (dalam arti patokan yang bersifat alamiah, atau sesuai dengan sifat-sifat alam).³⁰

Makna undang-undang secara etimologis tersebut hampir sama dengan makna undang-undang secara terminologis. Dalam kaitan ini menurut C.S.T. Kansil, undang-undang adalah “suatu peraturan negara yang mempunyai kekuatan hukum yang mengikat, diadakan dan dipelihara oleh penguasa negara.”³¹ Sedangkan menurut Byus, bahwa:

²⁸John M. Echols dan Hassan Shadily, *Kamus Inggris-Indonesia* (Cet. XXV; Jakarta: Gramedia Pustaka Utama, 2003), h. 155.

²⁹Secara kebahasaan *cyber crime* sering disamakan dengan “kejahatan mayantara” atau “kejahatan dunia maya”. Penjelasan lebih lanjut bisa dilihat dalam bukunya Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Cet. I; Bandung: Refika Aditama, 2005), h. 39.

³⁰Departemen Pendidikan Nasional R.I., *Kamus Besar Bahasa Indonesia* (Edisi 3, Cet. IV; Jakarta: Balai Pustaka, 2007), h. 1.245.

³¹C.S.T. Kansil, *Pengantar Ilmu Hukum dan Tata Hukum Indonesia* (Cet. VIII; Jakarta: Balai Pustaka, 1989), h. 46.

Undang-undang itu mempunyai dua arti, yakni:

- a. Undang-undang dalam arti formal, ialah setiap keputusan pemerintah yang merupakan undang-undang karena cara pembuatannya (misalnya dibuat oleh pemerintah bersama-sama dengan parlemen);
- b. Undang-undang dalam arti materiil, ialah setiap keputusan pemerintah yang menurut isinya mengikat langsung setiap penduduk.³²

Sedangkan yang dimaksud dengan Informasi dan Transaksi Elektronik menurut Undang-Undang ITE adalah:

Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), Surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.³³

- c. Hukum Pidana Islam

Sedangkan “Hukum Pidana Islam” merupakan terjemahan dari kata *fiqh jinayah*. *Fiqh jinayah* adalah segala ketentuan hukum mengenai tindak pidana atau perbuatan kriminal yang dilakukan oleh orang-orang *mukallaf* (orang yang dapat dibebani kewajiban), sebagai hasil dari pemahan atas dalil-dalil hukum yang terperinci dari Alquran dan hadis.³⁴ Tindakan kriminal yang dimaksud adalah tindakan-tindakan kejahatan yang mengganggu ketentraman umum serta tindakan melawan peraturan perundang-undangan yang bersumber dari Alquran dan hadis.

³²*Ibid.*, h. 46-47.

³³Redaksi New Merah Putih, *Undang-Undang ITE (Informasi dan Transaksi Elektronik)* (Cet. I; Yogyakarta; Penerbit New Merah Putih, 2009), h. 11.

³⁴Dede Rosyada, *Hukum Islam dan Pranata Sosial* (Jakarta: Lembaga Studi Islam dan Kemasyarakatan, 1992), h. 86.

Berdasarkan penjelasan tersebut, maka yang dimaksudkan dengan “*Cyber Crime* Menurut Undang-Undang ITE (Perspektif Hukum Pidana Islam)”, adalah kajian ilmiah mengenai kejahatan yang dilakukan oleh seseorang maupun kelompok dengan menggunakan sarana komputer, internet dan alat telekomunikasi lainnya menurut Undang-Undang ITE berdasarkan tinjauan hukum pidana Islam.

2. Ruang Lingkup Penelitian

Adapun ruang lingkup penelitian dalam tesis ini, adalah:

- a. Hakikat *cyber crime* dan eksistensinya dalam Undang-Undang ITE.
- b. Perspektif hukum pidana Islam tentang *cyber crime*.
- c. Bentuk sanksi pidana *cyber crime* menurut hukum pidana di Indonesia dan hukum pidana Islam.

D. Kajian Pustaka

Kajian tentang “*Cyber Crime* Menurut Undang-Undang ITE (Perspektif Hukum Pidana Islam)” sejauh penelusuran yang dilakukan terhadap sejumlah literatur belum pernah ditemukan. Namun sumber literatur yang membahas tentang penelitian ini dapat ditemukan dari beberapa tulisan baik yang berbahasa asing maupun berbahasa Indonesia dengan masing-masing aspek kajiannya. Di antara hasil penelitian yang relevan dengan penelitian ini adalah:

Abdul Wahid dan Mohammad Labib dalam bukunya berjudul “*Kejahatan Mayantara (Cyber Crime)*”. Buku tersebut mencoba menawarkan beberapa solusi dalam menghadapi fenomena berat dunia kriminalitas baru yang disebut *cyber crime*. Pendeskripsian dari sisi sosiologi hukum, kriminologi dan alternatif penerapan hukum. Hal ini dinilai kurang memadai apabila aspek-aspek pencegahan dini tidak

dipaparkan secara detail. Untuk itu, dirasa perlu memberikan penekanan pada aspek pencegahan dini.

Barda Nawawi Arief, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*, dalam buku ini tepatnya pada bab VIII diuraikan tentang penanggulangan *cyber crime* perspektif hukum pidana. Pada bab tersebut Barda Nawawi Arief mencoba menguraikan penanggulangan *cyber crime* dalam berbagai aspeknya, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian), dan aspek yurisdiksi.

Dalam kaitan ini, Barda Nawawi Arief hanya sekedar melihat dari aspek penanggulangan *cyber crime*. Sehingga pada aspek sosio-kultural yang menjadi pemicu munculnya *cyber crime* kurang tersentuh. Oleh karena itu, pada aspek tersebut dapat menjadi pertimbangan dalam kajian *cyber crime* ini.

Sedangkan Sutarman dalam bukunya *Cyber Crime Modus Operandi dan Penanggulangannya* cukup memberikan informasi baru dengan orientasi riset yang sama, meskipun aspek yang dilihatnya berbeda. Buku ini mencoba meneropong fenomena kejahatan di dunia maya (*cyber crime*) yang saat ini merajalela di Indonesia, sementara di sisi lain perangkat hukum pidana di Indonesia *out of date*, sehingga tidak optimal dalam menangani *cyber crime*. Hal inilah yang akan menjadi bagian dari fokus penelitian selanjutnya. Dalam kajian tersebut belum sepenuhnya terkaji secara utuh sekaligus menjadi pelengkap kajian lanjutan.

Agus Raharjo dalam bukunya, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* mencoba membuka tabir yang selama ini tertutup. *Cyber crime* yang dinilai sebagai kejahatan berteknologi, hadir karena

lahirnya teknologi informasi dan akan tetap ada bersama dengan keberadaan teknologi informasi (internet). Mengingat internet saat ini sudah dipakai oleh manusia pada hampir semua kegiatan, maka pencegahan dan penanggulangan *cyber crime* ini merupakan faktor yang tidak dapat ditunda-tunda lagi sehingga seseorang yang menggunakan dapat memanfaatkan internet dengan sebaik-baiknya tanpa ada perasaan was-was atau kekhawatiran terhadap pelaku *cyber crime*.

Sejalan dengan hal tersebut, Sutarman memaparkan pula bahwa pemahaman tentang kejahatan berteknologi atau dalam hal ini *cyber crime*, tidak cukup hanya mendasarkan pada teori-teori kriminologi, terutama teori kriminologi klasik. Pemahaman yang didasarkan pada pengertian yang komprehensif mengenai teknologi informasi/internet, sehingga pengertian kejahatan berteknologi itu tidak berat sebelah. Maksudnya tidak hanya memandang faktor manusia sebagai unsur utama dalam kejahatan berteknologi itu, tetapi juga melihat faktor lain seperti faktor teknologi, budaya, politik, sosial dan sebagainya sebagai unsur yang turut serta dalam terbentuknya kejahatan berteknologi.

Widodo dalam bukunya *Sistem Pemidanaan dalam Cyber Crime: Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan bagi Pelaku Cyber Crime* mencoba menguraikan secara argumentatif tentang pembenaran penggantian pidana pengawasan bagi pelaku *cyber crime*. Menurutnya, pidana penjara banyak kelemahan dan daya tampung Lembaga Pemasyarakatan di Indonesia sudah kelebihan beban, serta kapasitas dan kapabilitasnya tidak memenuhi syarat. Pada buku tersebut Widodo mencoba membidik tentang perlunya penerapan pidana kerja sosial dan pengawasan sebagai alternatif pengganti penjara pidana dalam *cyber crime*.

Dilihat dari orientasinya, pemidanaan tidak sekedar membebani pelaku kejahatan dengan hukuman sebagai pertanggungjawaban hukum, melainkan juga harus memiliki efek jera. Pembahasan buku tersebut sepatutnya melihat persoalan secara komprehensif agar tujuan pemidanaan dapat tercapai.

Buku-buku yang dipaparkan tersebut secara umum mengkaji pada domain hukum pidana di Indonesia dan tidak membahas aspek hukum pidana Islam. Oleh karena itu, penelitian ini mencoba memberi ruang pada aspek yang baru hukum pidana Islam.

Berdasarkan hasil kajian tersebut, maka yang menjadi fokus penulisan tesis ini tidak sekedar mendeskripsikan kajian *cyber crime*, tetapi juga mengeksplorasi pesan-pesan yang terkandung di dalam Undang-Undang ITE terhadap hukum pidana Islam dengan mengklasifikasikan dan mengategorikan pasal-pasal yang relevan dan sinkron terhadap hukum pidana Islam. Di samping itu, mencoba memformulasi *cyber crime* dalam hukum positif di Indonesia sehingga *cyber crime* yang terkandung di dalam undang-undang tersebut tergambar secara utuh berdasarkan dimensi yuridis.

E. Kerangka Teoretis

Penegakan hukum (*law an forcement*) merupakan permasalahan hampir di setiap negara, khususnya bagi negara-negara berkembang. Permasalahan hukum sangat banyak dan beragam baik kualifikasinya maupun modus operandinya. Banyaknya masalah hukum tersebut, maka banyak pula yang belum atau bahkan mungkin sulit untuk dapat diselesaikan. Salah satu masalah yang masih melilit adalah *cyber crime*. Permasalahan hukum tersebut terjadi secara kompleks dan sistemik. Oleh karena itu, pembenahannya pun juga harus dilakukan secara sistemik.

Menurut Friedman, sistem hukum mencakup tiga aspek yaitu: aspek struktural, substansial dan kultural. Agar supremasi hukum dapat terwujud, tentunya ketiga sub sistem tersebut harus dilakukan secara simultan. Struktur hukum yang dimaksud di sini mencakup dua hal, yaitu kelembagaan hukum dan aparatur hukum. Substansi hukum adalah norma hukum, sedangkan kultur hukum adalah bagaimana hukum itu dilaksanakan dalam kehidupan masyarakat.³⁵

Secara teoretis, hukum berfungsi untuk menciptakan keadilan, keamanan dan ketentraman hidup dalam masyarakat. Demikian pula hukum pidana Islam bertujuan untuk memberikan perlindungan dan pengayoman bagi masyarakat demi tegaknya keadilan dan kebenaran. Hal ini sejalan dengan peran hukum, termasuk hukum pidana Islam, sebagai *social control (social change)* yang menjadi bagian dari sistem yang mengintegrasikan individu ke dalam masyarakat dan sebagai *social engeneering (a tool of social engeneering)* yang merupakan sarana penegakan masyarakat yang ditujukan untuk mengubah perilaku warga masyarakat sesuai dengan tujuan yang ditentukan.³⁶

Sejalan dengan fungsi hukum sebagai kontrol sosial, *cyber crime* menjadi titik sentral kajian dalam upaya memformulasikan hukum di Indonesia dengan fokus kajian Undang-Undang ITE. Bertolak dari undang-undang tersebut mencoba mengeksplorasi untuk memperoleh relevansinya terhadap hukum pidana Islam.

Secara substansial hukum dibuat berorientasi kepada kemaslahatan dan mencegah kejahatan manusia. Islam memperkenalkan suatu konsep sebagai kerangka

³⁵M. Lawrence Friedman, *Law and Society: An Introduction* (Englewood Cliff: Prentice Hall Inc., 1977), h. 71-74.

³⁶Lihat Todung Mulya Lubis, *Hak Asasi Manusia dan Pembangunan* (Jakarta: YLBHI, 1987), h. 21.

teoretis berupa teori *al-maslahah* dalam menanggulangi kejahatan tersebut dilihat dari sisi kekuatan substansinya, baik pada tataran *dharuriyat* (primer, sangat utama), atau berada pada tingkat *hajiyyat* (sekunder, kebutuhan) dan berada pada tingkat *tahsiniiyat* (tersier, kebaikan).³⁷ Kemaslahatan *dharuriyat* yaitu kemaslahatan yang harus ada untuk tegaknya kebahagiaan, kemaslahatan bagi manusia, baik ukhrawiyah maupun *dunyawiyah*, dalam arti apabila *dharuriyat* tidak ditegakkan, maka akan terganggu keharmonisan kehidupan manusia di dunia ini dan akan hilang kenikmatan serta akan mendapatkan siksa di akhirat dan merupakan suatu kerugian yang nyata. Kemaslahatan *hajiyyat* yaitu segala sesuatu yang dibutuhkan oleh manusia untuk menghindari *musyaaqqat* guna membuat ringan dan lapang serta menghindari kepayahan-kepayahan dalam mengarungi kehidupan. Sedangkan kemaslahatan *tahsiniiyat* yaitu mempergunakan segala yang layak dan pantas yang ada dalam adat kebiasaan yang baik, semuanya dicakup oleh bagian penyempurnaan akhlak, atau sesuatu yang dituntut oleh norma dalam tatanan hidup serta berperilaku menurut jalan yang lurus.³⁸

Hal tersebut sejalan dengan teori *maqasid al-syari'ah*. Prinsip *maqasid al-syari'ah* adalah kemaslahatan umat manusia.³⁹ Kemaslahatan itu dengan menggunakan analisis *maqasid al-syari'ah* tidak hanya dilihat dalam arti teknis belaka, akan tetapi dalam upaya dinamika dan pengembangan hukum dilihat sebagai sesuatu yang mengandung nilai filosofis dari hukum-hukum yang disyariatkan

³⁷Andi Hamzah, *Asas-asas Hukum Pidana*, Edisi Revisi (Jakarta: Renika Cipta, 1994), h. 28 dalam Sabri Samin, *Pidana Islam dalam Politik Hukum Indonesia Eklektisisme dan Pandangan Non Muslim* (Cet. I; Jakarta: Kholam Publishing, 2008), h. 31.

³⁸Syamsul Bahri, *Metodologi Hukum Islam* (Cet. I; Yogyakarta: TERAS, 2008), h. 93-96.

³⁹Abu Ishak al-Syatibi Ibrahim bin Musa al-Garnati al-Maliki, *al-Muwafaqat fi Ushul al-Syari'ah*, Jilid II (Beirut: Dar al-Kutub al-'Ilmiyyah, [t.th.]), h. 4.

Tuhan kepada manusia. Oleh karena itu, pengetahuan dan pemahaman *maqasid al-syari'ah* dari Alquran dan sunnah nabi sebagai sumber pencarian *maqasid al-syari'ah* merupakan aspek penting dalam melakukan *istinbat hukum*.⁴⁰

Dilihat dari aspek yuridis, teori *maqasid al-syari'ah* meletakkan prinsip-prinsip yang menjadi pertimbangan pokok dari tujuan hukum, yaitu terwujudnya kemaslahatan manusia baik di dunia maupun di akhirat, yaitu terwujud dan terpeliharanya *al-masalih al-khamsah* atau lima kebutuhan pokok dalam kehidupan manusia yang mencakup pemeliharaan agama (*hifz al-din*), jiwa (*hifz al-nafs*), keturunan atau kehormatan (*hifz al-nasl*), harta (*hifz al-mal*) dan akal (*hifz al-'aql*).⁴¹

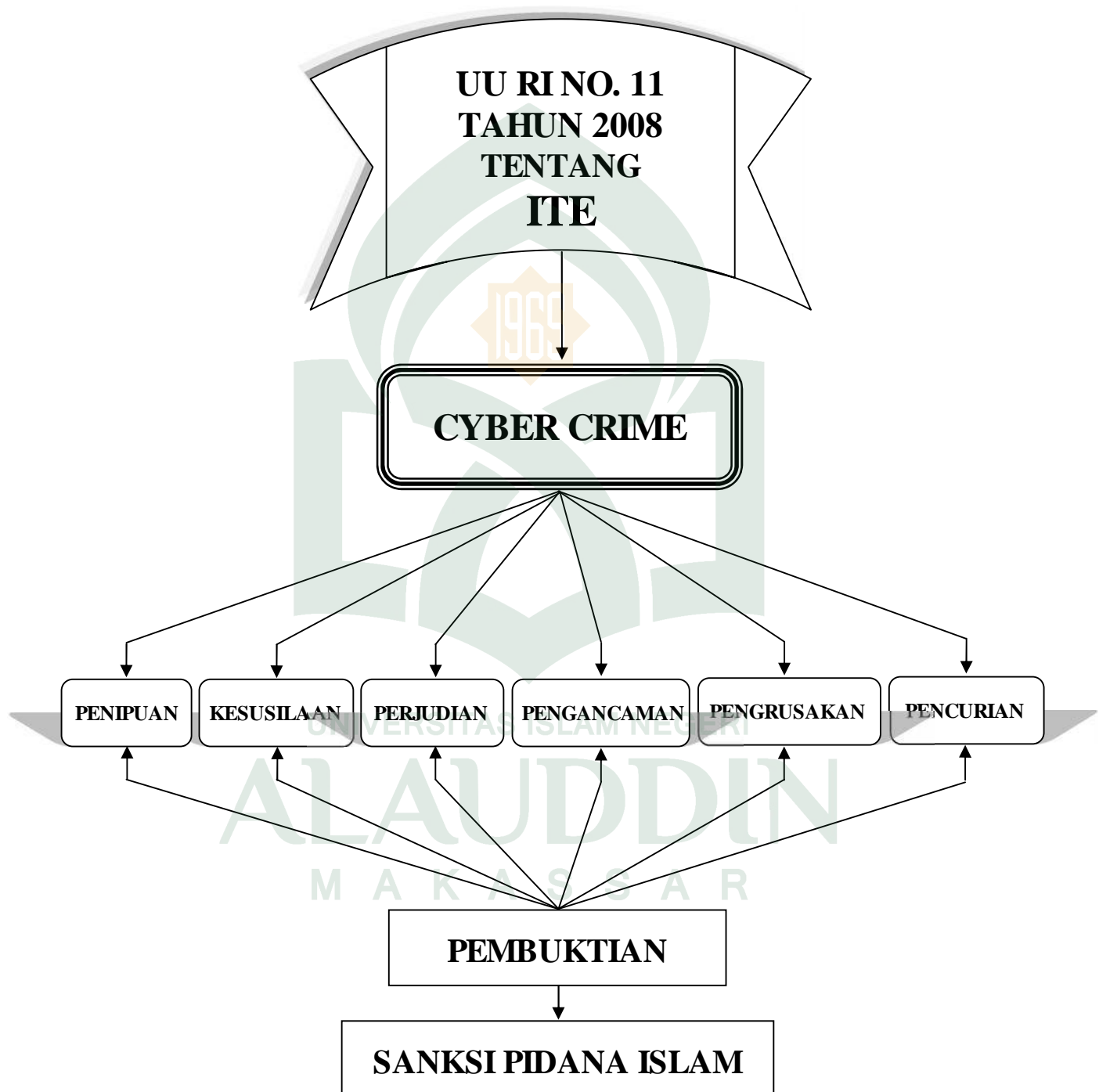
Dengan demikian kejahatan merupakan suatu fenomena kompleks yang dapat dipahami dari berbagai sisi yang berbeda. Hal itulah sebabnya dalam keseharian seseorang dapat menangkap berbagai komentar tentang suatu peristiwa kejahatan yang berbeda satu dengan yang lain, baik kejahatan itu dilakukan di dunia nyata maupun di dunia maya. Fenomena *cyber crime* juga menjadi bagian kejahatan yang dilakukan di dunia maya (*virtual*). Karena kejahatan tidak mengenal waktu dan tempat, maka kejahatan di manapun dan kapanpun pada dasarnya memiliki implikasi yang sama, hanya memiliki sedikit perbedaan tingkat kadar yang diakibatkannya.

Cyber crime sebagaimana yang terkandung dalam Undang-Undang ITE yang tidak ubahnya sebagai dunia maya tetapi nyata, yang tentunya memiliki korelasi yang sama dengan hukum pidana Islam.

Berdasarkan uraian tersebut, maka kerangka pikir dalam penelitian ini dapat digambarkan sebagai berikut:

⁴⁰Syamsul Bahri, *op. cit.*, h. 105.

⁴¹Al-Syatibi, *op. cit.* Jilid I, Juz I, h. 195.

SKEMA KERANGKA PIKIR

F. Metodologi Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian kualitatif eksplanatif terhadap permasalahan *cyber crime* di Indonesia dalam Undang-Undang ITE.

2. Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini adalah:

a. Pendekatan Teologis Normatif (*syar'i*)

Pendekatan *syar'i* digunakan untuk menganalisis ketentuan-ketentuan hukum pidana Islam yang bersumber dari Alquran, hadis dan pendapat ulama mengenai kejahatan dunia maya (*cyber crime*).

b. Pendekatan Yuridis Normatif (*normative statue approach*)

Pendekatan yuridis normatif digunakan untuk menganalisis berbagai ketentuan dalam Undang-Undang ITE. Undang-undang tersebut dapat dipandang sebagai sumber yuridis terhadap kejahatan dunia maya (*cyber crime*).

c. Pendekatan Sosiologis (*sociological approach*)

Pendekatan sosiologis untuk menganalisis berbagai fenomena atau gejala sosial yang berkaitan dengan *cyber crime*. Pendekatan sosiologis digunakan untuk menelusuri aspek eksternal sanksi pidana dari *cyber crime*. Meskipun penelitian ini murni kajian teks dalam undang-undang sebagaimana tersebut, penelitian ini diharapkan memberikan gambaran lebih komprehensif.

d. Pendekatan Historis (*historical approach*)

Pendekatan historis adalah prosedur pemecahan masalah dengan menggunakan data masa lalu atau peninggalan-peninggalan, baik untuk memahami kejadian atau suatu keadaan yang berlangsung pada masa lalu terlepas dari

keadaan masa sekarang dalam hubungannya dengan kejadian atau keadaan masa lalu, selanjutnya sering kali juga hasilnya dapat dipergunakan untuk meramalkan kejadian atau keadaan masa yang akan datang.⁴² Pendekatan ini digunakan untuk membantu peneliti untuk mengetahui dan memahami sejarah perkembangan *cyber space* dan memahami munculnya *cyber crime* dari waktu ke waktu.

3. Pengumpulan Data

Untuk memperoleh data yang dibutuhkan dalam penulisan tesis ini, penulis menggunakan penelitian kepustakaan (*library research*). Penelitian kepustakaan digunakan untuk mendapatkan teori-teori dari literatur-literatur yang telah diakui kualitasnya. Data-data tersebut dikumpulkan, baik data primer maupun data sekunder. Selanjutnya, data-data tersebut dikutip menggunakan kutipan langsung maupun kutipan tidak langsung.

4. Pengolahan dan Analisis Data

Penelitian ini merupakan penelitian kualitatif eksplanatif yang menghasilkan data deskriptif, sehingga memerlukan pendekatan deskriptif analisis. Oleh karena itu, kajian ini pada dasarnya mencoba mengeksplorasi isi undang-undang yang menyangkut *cyber crime*. Undang-undang yang dimaksud adalah Undang-Undang ITE, yang seutuhnya menghendaki telaah terhadap karya-karya tertulis dari para pakar dalam bidang hukum Islam. Dengan demikian ia merupakan penelitian pustaka (*library research*) yang dapat diperoleh melalui data kepustakaan khususnya yang berkaitan dengan hukum kejahatan mayantara (*cyber crime*) dan hukum pidana Islam. Penelitian kualitatif eksplanatif ini diarahkan pada studi teks yang

⁴²Hadari Nawawi, *Metode Penelitian Bidang Sosial* (Cet. VIII; Yogyakarta: Gajah Mada University Press, 1998), h. 79.

mengkorelasikan antara hukum pidana dalam Undang-Undang ITE dan hukum pidana Islam. Penulis mencoba menjelaskan secara mendalam untuk mencari titik temu dari keduanya dengan melihat kesamaan unsur dan ciri-ciri yang terkandung di dalamnya.

Untuk mendukung kajian tersebut dilengkapi dengan analisis ilmiah tentang isi pesan suatu komunikasi melalui *content analysis* yang mempunyai tiga syarat yaitu obyektifitas, sistematis dan generalisasi. Obyektifitas dengan berlandaskan aturan yang dirumuskan secara eksplisit. Sistematis, karena kategorisasi isi harus menggunakan kriteria tertentu. Sedangkan generalisasi artinya temuannya haruslah mempunyai sumbangan teoretik. *Content analysis* ini dipandu dengan menggunakan pendekatan transdisipliner yang menyatukan pendekatan interdisipliner dan multidisipliner dengan studi Islam teologik. Pada akhirnya *cyber crime* juga merupakan bagian dari keseluruhan hukum pidana Islam dengan melihat kesamaan unsur dan ciri-cirinya. Di samping itu, digunakan pula studi kontekstual dengan tiga model. *Pertama*, kontekstual sebagai upaya pemaknaan menanggapi masalah kini yang umumnya mendesak (situasional). *Kedua*, kontekstual dengan melihat keterkaitan masa lampau, kini dan mendatang. Dalam hal ini uraian akan memperhatikan makna historik dahulu, makna fungsional sekarang dan memprediksikan atau mengantisipasi makna kemudian hari. *Ketiga*, pemaknaan kontekstual berarti mendudukan keterkaitan antara yang sentral dengan yang perifer.⁴³

⁴³Lihat Noeng Muhadjir, *Metodologi Penelitian kualitatif*, Edisi ketiga (Cet. Ke-7; Yogyakarta: Rake Sarasin, 1996), h. 178.

Adapun teknik interpretasi data dengan berpikir induktif seperti argumentasi, kausalitas atau perbandingan dan berpikir deduktif seperti analogi terjadi secara reflektif dan terus menerus selama proses menuangkan pikiran-pikiran dan hasil bacaan berlangsung. Namun pemahaman intelektual dan kemampuan berargumentasi secara logik perlu didukung dengan data empirik yang relevan agar produk ilmu yang melandaskan diri pada rasional adalah ilmu bukan fiksi.⁴⁴

Langkah-langkah yang dilakukan dalam penulisan tesis ini dengan cara mengidentifikasi, mereduksi data⁴⁵, mengklasifikasikan dan mengategorikan pasal-pasal yang masuk dalam kategori pidana untuk dikorelasikan dengan hukum pidana Islam dengan melihat kesamaan unsur-unsur dan ciri-cirinya yang terkandung di dalam pasal-pasal tersebut. Sesudah itu diinterpretasi dan dianalisis kemudian disimpulkan berdasarkan pemaknaan.

G. Tujuan dan Kegunaan Penelitian

1. Tujuan Penelitian

Penelitian ini bertujuan:

- a. Untuk mengetahui hakikat *cyber crime* dan eksistensinya dalam Undang-Undang ITE.
- b. Untuk mengetahui *cyber crime* menurut perspektif hukum pidana Islam.
- c. Untuk mengetahui bentuk sanksi pidana *cyber crime* menurut hukum pidana di Indonesia dan hukum pidana Islam.

⁴⁴*Ibid.*, h. 37.

⁴⁵Reduksi data yaitu proses pemilihan, pemusatan perhatian untuk menyederhanakan, mengabstraksikan dan memformulasi data kasar yang diperoleh.

2. Kegunaan Penelitian

a. Kegunaan Teoretis

1) Hasil penelitian ini diharapkan dapat memberikan informasi baru tentang unsur-unsur kriminalisasi *cyber crime* berdasarkan yuridis.

2) Hasil penelitian ini diharapkan dapat memberikan kontribusi positif terhadap ilmu hukum yang berkaitan dengan *cyber crime* dan mengetahui lebih mendalam tentang pembuktian-pembuktiannya. Mengingat kajian *cyber crime* belum terlalu meluas dan belum banyak dikaji di kalangan akademik, sehingga harapannya hasil penelitian ini mampu menjadi pelengkap terhadap kajian hukum pidana menyangkut *cyber crime*.

3) Hasil penelitian ini diharapkan dapat memberikan nilai kontribusi positif terhadap khasanah ilmu hukum Islam, terutama konsep-konsep fikih yang berkaitan dengan hukum pidana Islam. Di samping itu, sebagai langkah lanjutan dalam pengkajian hukum pidan Islam pada aspek *cyber crime* di Indonesia, sehingga hukum pidana Islam mampu menyorot *cyber crime* sebagai bagian yang tidak terpisahkan dari objek kajian hukum yang senantiasa relevan dengan perubahan zaman, waktu, kondisi dan budaya.

b. Kegunaan Praktis

1) Hasil penelitian ini diharapkan dapat menjadi sumbangan pemikiran dalam penanggulangan *cyber crime* di Indonesia.

2) Hasil penelitian ini diharapkan dapat menjadi salah satu upaya merekonstruksi gagasan fikih jinayah atau hukum pidana Islam menyangkut *cyber crime*. Mengingat perkembangan internet yang sangat meluas dipergunakan oleh masyarakat Indonesia ternyata juga ikut andil dalam memfasilitasi para pengguna

internet dalam melakukan kejahatan. Oleh karena itu, hukum Islam diharapkan mampu melihat sanksi pidana *cyber crime* dalam hukum pidana Islam.

H. Garis Besar Isi Tesis

Untuk mendapatkan gambaran tesis ini, akan dijelaskan secara garis besar. Tesis ini terdiri dari lima bab dengan garis besar sebagai berikut:

Bab pertama, pendahuluan. Dalam bab ini diuraikan tentang hal-hal yang melatarbelakangi pengangkatan judul ini. Setelah latar belakang tersebut dijelaskan, kemudian merumuskan masalahnya. Untuk menghindari pengertian yang bersifat *ambivalens*, dijelaskan definisi operasional dari judul tesis ini. Selanjutnya, kajian pustaka, untuk mendemonstrasikan hasil bacaan terhadap buku-buku atau hasil penelitian terdahulu yang relevan dengan masalah yang diteliti, serta kemungkinan signifikansi dan kontribusi akademik. Paparan dan pendalaman teori terhadap kajian ini digunakan sebagai dasar atau pijakan dalam menganalisis. Hal lain yang berkaitan dengan metodologi penelitian, serta tujuan dan kegunaan penelitian dipaparkan dalam bab ini. Sebagai penutup bab, diuraikan garis besar isi tesis.

Bab kedua, membahas tentang tinjauan umum *cyber crime*. Pada bab ini akan diuraikan landasan teori yang berisi tentang kajian teoretis mengenai pengertian *cyber crime*, kemudian menguraikan jenis-jenis *cyber crime*. Selanjutnya memaparkan sejarah *cyber crime* dan ruang lingkup *cyber crime*.

Bab ketiga, membahas tentang konsepsi *cyber crime* dalam hukum pidana di Indonesia. Uraian dalam bab ini menyangkut hakikat *cyber crime* dan eksistensinya dalam Undang-Undang ITE, faktor-faktor yang memengaruhi *cyber crime*, modus operandi terjadinya *cyber crime*, penanggulangan *cyber crime* berdasarkan

perundang-undangan di Indonesia, unsur-unsur pidana dalam *cyber crime*, pembuktian *cyber crime* dalam hukum pidana di Indonesia dan sanksi pidana bagi pelaku *cyber crime*. Pembahasan dalam bab ini diharapkan dapat memberikan landasan yang kuat dalam menganalisis permasalahan yang dibahas dalam bab keempat.

Bab keempat, membahas analisis *cyber crime* dalam perspektif hukum pidana Islam dengan mencari akar *cyber crime* dalam Islam. Dalam bab ini diuraikan tentang perspektif hukum pidana Islam tentang *cyber crime*, *cyber crime* dan relevansinya dengan jarimah, *cyber crime* dan korelasinya dalam pembagian hukum pidana Islam serta pembuktian *cyber crime* dalam hukum pidana Islam dan sanksi pidana *cyber crime* dalam hukum pidana Islam. Pembahasan dalam bab ini diharapkan dapat menjawab sub masalah pertama, kedua dan ketiga dalam tesis ini.

Berdasarkan pembahasan dalam bab-bab sebelumnya, maka dalam bab kelima dirumuskan beberapa kesimpulan dan rekomendasi penelitian yang relevan dengan permasalahan yang dibahas.

BAB II

TINJAUAN UMUM *CYBER CRIME*

A. Pengertian Cyber Crime

Berdasarkan hasil penelusuran, pengertian *cyber crime* belum terdefinisi secara baku. Mengingat pengertian yang dikemukakan oleh para pakar sangat beraneka ragam, tetapi pengertian yang satu dengan yang lain saling melengkapi. Oleh karena itu, penting untuk dipaparkan pengertiannya.

Secara etimologi *cyber crime* berasal dari dua rangkaian kata, yaitu *cyber* dan *crime*. Menurut Kamus Bahasa Inggris-Indonesia *cyber* berarti maya, sedangkan *crime* diartikan dengan kejahatan.¹ Menurut *Dictionary of Contemporary English*, *crime* adalah *an offence which is punishable by law* (suatu kejahatan yang dihukum oleh hukum), *illegal activity in general* (kegiatan ilegal pada umumnya), atau *a bad, immoral, or dishonourable act* (tidak terhormat, tidak bermoral, atau tindakan yang buruk).² Secara kebahasaan *cyber crime* samakna dengan “kejahatan dunia maya” atau “kejahatan mayantara”.³

Sedangkan menurut terminologi, akan dikemukakan berdasarkan pendapat para pakar sebagai berikut:

¹John M. Echols dan Hassan Shadily, *Kamus Inggris-Indonesia* (Cet. XXV; Jakarta: Gramedia Pustaka Utama, 2003), h. 155.

²Longman Group, *Longman dictionary of Contemporary English* (Ed. VIII; England: [t.tp], 1998), h. 155.

³Secara kebahasaan *cyber crime* sering disamakan dengan “kejahatan mayantara” atau “kejahatan dunia maya”. Penjelasan lebih lanjut bisa dilihat dalam bukunya Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Cet. I; Bandung: Refika Aditama, 2005), h. 39.

Cyber crime adalah kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet.⁴ Berdasarkan pengertian tersebut terlihat bahwa *cyber crime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet.⁵ Definisi ini tidak menyebutkan secara spesifik dari karakteristik *cyber crime*. Definisi ini mencakup segala kejahatan yang dalam modus operandinya menggunakan fasilitas internet.

Menurut Kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.⁶

Berdasarkan dari definisi tersebut yang menjadi catatan adalah bahwa dalam definisi tersebut tidak dijelaskan apa maksud kata “jaringan komputer”⁷. Apabila dimaknai secara luas, maka akan meliputi LAN (*local area networking*)⁸ dan

⁴<http://www.thecelia.com/dokumen/jurnal/ajo.a002.shtml>. (Diakses pada tanggal 25 Juni 2010)

⁵Internet (*international-networking*) adalah jaringan luas dari komputer yang lazim disebut dengan *Worldwide Network*. Internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik, satelit ataupun gelombang frekuensi. Jaringan komputer ini dapat berukuran kecil seperti *Lokal Area Networking* (LAN) yang biasa dipakai secara intern di kantor-kantor, bank, perusahaan atau biasa disebut dengan intranet, dapat juga berukuran superbesar (internet).

⁶Lihat Abdul Wahid dan Mohammad Labib, *op. cit.*, h. 40.

⁷Menurut Institut Komputer Indonesia, komputer didefinisikan sebagai berikut: “Komputer adalah suatu rangkaian peralatan-peralatan dan fasilitas yang bekerja secara elektronis, bekerja di bawah kontrol suatu *operating system*, melaksanakan pekerjaan berdasarkan rangkaian instruksi-instruksi yang disebut program serta mempunyai internal *storage* yang digunakan untuk menyimpan *operating system*, program dan data yang diolah.” Lihat Institut Komputer Indonesia (IKI), *Pengenalan Komputer (introduction to computer)*, (Jakarta: [t.p.], 1981), h. 1. Sedangkan jaringan komputer adalah rangkaian beberapa komputer dari suatu tempat atau ruangan atau gedung yang bekerja dalam suatu sistem komunikasi elektronis.

⁸LAN (*Local Area Networking*) adalah cara menghubungkan sejumlah komputer melalui saluran komunikasi sehingga dapat saling berbagi data dan peralatan pendukung. Lihat *Kamus Lengkap Dunia Komputer* (Edisi I; Yogyakarta: Andi Yogyakarta dan Wahana Komputer Semarang, 2002), h. 223.

internet. LAN ini mempunyai karakter yang berbeda dengan internet. LAN merupakan jaringan tertutup. Dalam beberapa segi, jenis kejahatan yang disebut termasuk dalam katagori *cyber crime* tidak dapat dilakukan dalam LAN ini, seperti *spamming*,⁹ *cybersquatting*,¹⁰ *typosquatting*.¹¹

Menurut beberapa literatur, *cyber crime* sering diidentikkan dengan *computer crime*. *The US Department of Justice* memberikan pengertian *computer crime* sebagai “any illegal act requiring knowledge of computer for it’s perpetration, investigation, or prosecution”, artinya “setiap perbuatan melanggar hukum yang memerlukan pengetahuan tentang komputer untuk menangani, menyelidiki dan menuntutnya”.¹²

Sementara pengertian lainnya diberikan oleh *Organization of European Community Development*, yaitu: “any illegal, unethical or unauthorized behaviour relating to the automatic processing and/or the transmission of data”, artinya “setiap perilaku ilegal, tidak pantas, tidak mempunyai kewenangan yang berhubungan dengan pengolahan data dan/atau pengiriman data”.¹³

⁹*Spamming* adalah kegiatan mengirimkan *e-mail* sampah (tidak berguna) secara serentak ke sejumlah besar alamat *e-mail*. Umumnya merupakan *e-mail* yang berisi iklan suatu produk. Lihat Tim Andi Yogyakarta dan Wahana Komputer Semarang. *Kamus Lengkap Dunia Komputer* (Edisi I; Yogyakarta: Andi Yogyakarta dan Wahana Komputer Semarang, 2002), h. 419.

¹⁰*Cybersquatting* adalah kejahatan yang berhubungan dengan nama domain. Nama domain (*domain name*) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan nama domain perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Lihat Budi Raharjo dalam www.cert.or.id/~budi/articles/cybercrime.doc (Diakses pada tanggal, 25 Juli 2010).

¹¹*Typosquatting* adalah domain plesetan atau domain yang mirip dengan nama domain orang lain. Seperti, kasus klikbca.com. Masalah lain adalah menggunakan domain saingan perusahaan untuk merugikan perusahaan lain. Misalnya, kasus: mustikaratu.com. Lihat *Ibid*.

¹²Ari Juliano Gema, *op. cit*.

¹³*Ibid*.

Indra Safitri mengemukakan, *cyber crime* (kejahatan dunia maya) adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.¹⁴

Menurut laporan kongres PBB X/2000 dinyatakan *cyber crime* atau *computer-related crime*, mencakup keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan pada komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer.¹⁵

Muladi dalam bukunya yang ditulis bersama Barda Nawawi Arief, "*Bunga Rampai Hukum Pidana*" memandang *cyber crime* dengan pendekatan *computer crime* (kejahatan komputer). Namun demikian, *cyber crime* sesungguhnya berbeda dengan *computer crime*.¹⁶

¹⁴http://business.fortunecity.com/buffett/842/art180199_tindak_pidana.htm. (Diakses pada tanggal, 25 Juni 2010)

¹⁵Lihat Barda Nawawi Arief, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan* (Cet. I; Bandung: PT Citra Aditya Bakti, 2005), h. 136. Lihat juga dalam Dokumen Kongres PBB X, A/CONF.187/L.10, 16-4-2000, h. 1-2 dan dokumen A/CONF.187/15, 19-7-2000, h. 26:

"the entirely new forms of crime that were directed at computers, networks and their users, and the more traditional form of crime that were now being committed with the use or assistance of computer equipment".

"format kejahatan baru yang telah diarahkan pada komputer, jaringan dan para pemakai mereka, dan format kejahatan tradisional yang kini sedang dilakukan dengan penggunaan atau bantuan peralatan komputer".

¹⁶Agus Raharjo, *op. cit.*, h. 228.

Meskipun demikian, ada upaya untuk memperluas pengertian komputer agar dapat melingkupi segala kejahatan di internet dengan peralatan apapun, seperti pengertian komputer dalam *The Proposed West Virginia Computer Crimes Act*;

an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or type-setter, a portable hand-held calculator, or other similar device". (peralatan pemrosesan data listrik, magnetik, optik, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau tipe-setter, sebuah kalkulator tangan atau peralatan serupa lainnya).¹⁷

Dengan demikian, pendapat yang mengidentikkan *cyber crime* dengan *computer crime* dapat dipahami dengan menggunakan pendekatan pemaknaan komputer yang diperluas seperti pengertian tersebut di atas.

Pengertian yang membedakan antara *cyber crime* dengan *computer crime* diajukan oleh Nazaru Abdul Manap sebagai berikut:

Defined broadly, "computer crime" could reasonably include a wide variety of criminal offences, activities or issues. It also known as a crime committed using a computer as tool and it involves direct contact between the criminal and the computer. For instance, a dishonest bank clerk who unauthorisedly transfers a costumer's money to dormant account for his own interest or a person without permission has obtained acces to other person's computer directly to download information, which in the first place, are confidential. Tehe situations require direct access by the hacker to the victim's computer. There is no Internet line involved. Or only limited networking used such as the local area network (LAN).

Whereas, cyber-crimes are crimes committed virtually through internet online. This means that the crimes committed could extend to other countries, which is beyond the Malaysian jurisdiction. Anyway, it causes no harm to refer

¹⁷Ari Juliano Gema, *op. cit.*

computer crimes as cybercrimes or vice versa, since they have same impact in law.

Maksudnya adalah didefinisikan secara luas, kejahatan komputer dapat meliputi lingkup luas bermacam-macam pelanggaran, aktivitas atau isu kriminal. Ini dikenal dengan kejahatan yang dilakukan dengan komputer sebagai alat dan melibatkan hubungan langsung antara kriminal dan komputer. Contoh sebuah pegawai bank yang tidak jujur yang secara tidak sah mentransfer uang konsumen kepada akun-tidur untuk kepentingannya sendiri atau orang yang tanpa izin memperoleh akses terhadap komputer orang lain secara langsung untuk men-*download* informasi, yang pertama kali adalah terpercaya. Situasi ini membutuhkan akses langsung oleh *hacker* kepada komputer korban. Tidak ada saluran internet yang terlibat atau hanya menggunakan jaringan terbatas seperti LAN (*local area network*).

Di mana kejahatan *cyber* adalah kejahatan yang dilakukan secara *virtual* (maya) melalui internet *on line*. Ini berarti bahwa kejahatan yang dilakukan dapat berkembang ke negara lain yang berada di luar yurisdiksi Malaysia. Meskipun demikian, ini tidak dapat menyebabkan kejahatan *computer* sebagaimana kejahatan *cyber* atau sebaliknya, ketika mereka mempunyai dampak sama di dalam hukum.¹⁸

Dilihat dari beberapa definisi tersebut terlihat bahwa belum ada kesepakatan mengenai definisi tentang *cyber crime* atau kejahatan dunia *cyber*, sebagaimana yang dikatakan oleh Muladi, “Sampai saat ini belum ada definisi yang seragam tentang *cyber crime* baik secara nasional maupun global. Kebanyakan masih menggunakan *soft law* berbentuk *code of conduct* seperti di Jepang dan Singapura”.¹⁹

Ungkapan senada juga dinyatakan oleh Agus Raharjo, bahwa istilah *cyber crime* sampai saat ini belum ada kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cyber crime* dengan *computer crime*.²⁰

¹⁸ Agus Raharjo, *op. cit.* h. 227.

¹⁹ <http://www.suaramerdeka.com/harian/0207/24/nas13.htm>. (Diakses pada tanggal 25 Juni 2010)

²⁰ Agus Raharjo, *op. cit.*, h. 227.

Barda Nawawi Arief menggunakan istilah “tindak pidana mayantara” untuk menyebut *cyber crime*. Barda Nawawi Arief mengatakan, dengan istilah “tindak pidana mayantara” dimaksudkan identik dengan tindak pidana di ruang *cyber (cyber space)*²¹ atau yang biasa juga dikenal dengan istilah “*cyber crime*”.²²

Meskipun demikian, dapat dikemukakan rumusan definisi yang tidak jauh substansinya dari pengertian yang disebutkan oleh para pakar tersebut. Hal ini dimaksudkan sebagai bentuk ketegasan dalam menarik benang merah dari perbedaan yang ada, sehingga pengertian *cyber crime* tergambar secara jelas dan mudah dipahami.

Berdasarkan penjelasan tersebut, maka yang dimaksudkan dengan *cyber crime* adalah kejahatan yang dilakukan oleh seseorang, kelompok maupun korporasi dengan menggunakan sarana komputer dan alat telekomunikasi lainnya seperti *hand phone* sebagai dampak negatif dari perkembangan aplikasi internet.

B. Jenis-Jenis Cyber Crime

Dalam realitasnya, penyalahgunaan internet dapat dilakukan dengan berbagai macam dan cara. Berikut ini akan diuraikan beberapa jenis-jenis *cyber crime*, seperti kejahatan dalam *e-commerce*, *cyber sex*, *hacker*, dan merusak situs milik negara sebagaimana yang diuraikan oleh Sutarman.

²¹*Cyber space* (ruang maya) adalah terhubungnya komputer dengan saluran penyedia jasa internet yang dapat diakses kapan saja, tidak mengenal batas ruang dan waktu. Akses dapat dilakukan untuk transaksi jual beli barang, tukar informasi, mencari informasi atau bahkan merusak suatu jaringan komputer yang digelar oleh siapapun, baik pemerintah maupun swasta.

²²Barda Nawawi Arief, *Kapita Selekta Hukum Pidana* (Bandung: Citra Aditya Bakti, 2003), h. 239.

1. *E-Commerce*

Kegiatan perdagangan yang dilakukan melalui layanan elektronik, dalam hal ini melalui sarana internet, baik sistem promosi, sistem transaksi, sistem pembayaran. Landasan yang dipakai adalah *elektronik based* dan *information technology*, khususnya internet dan *website*.

Dengan hadirnya *e-commerce*, perdagangan dapat dilakukan sangat efektif, karena publik dapat mengakses suatu toko dari rumah masing-masing, tanpa harus memasuki toko atau perusahaan tersebut. *Website* perusahaan dapat dianggap sebagai sebuah toko, karena dalam *website* itu tersedia ruangan-ruangan maya yang menyediakan layanan spesifikasi barang-barang yang diperdagangkan. Adapun kejahatan dalam *e-commerce* seperti:

a. Pembobolan kartu kredit melalui internet

Tersangka Petrus Pangkur alias Bony Diobok-Obok, yang diputus oleh Pengadilan Negeri Sleman dengan hukuman penjara satu tahun penjara, dalam Perkara Nomor: 94/Pid.B/2002/PN.SLMN, tanggal 23 Agustus 2002, dalam perkara Tindak Pidana Penipuan dan atau Pemalsuan, pada tanggal 1 Maret 2001 dengan memesan barang berupa helm, sarung tangan melalui *e-commerce* dengan *account* kenny-jri@donet.com dan bonz.2000@cos.com, dan melakukan pembayaran dengan kartu kredit milik orang lain yang diperoleh dengan *carding* atas kartu kredit VSA nomor: 4388.5750.4013.3006, dan tersangka pada tanggal 8 Maret menerima kiriman barang yang dipesan itu melalui jasa paket UPS Yogyakarta.²³

²³Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya* (Cet. I; Yogyakarta: Laksbang Pressindo, 2007), h. 64.

b. Pemelesetan www.klikbca.com

Pada bulan Juni 2001, Steven Haryono membuat gempar dunia Teknologi Informasi (TI) Indonesia, dengan kasus pemelesetan www.klikbca.com. Motivasinya sebenarnya adalah untuk membuat kita semua tercengang terhadap masalah keamanan internet khususnya internet banking.²⁴

Adapun motif kejahatan yang terjadi dalam komunitas *e-commerce* ini, bisa berbentuk pemalsuan kartu kredit, persaingan usaha tidak sehat, monopoli barang perdagangan, HaKI.

2. *Cyber Sex*

Cyber sex adalah dunia pornografi yang dilakukan di internet, yang dapat diakses secara bebas. Situs ini dapat diakses dengan bebas, meskipun mereka yang mengakses ini belum cukup umur. Di kafe internet atau di penyedia layanan internet lainnya tidak ada aturan pembatasan umur, pembatasan akses dan aturan lain yang membatasi akses yang negatif.

Dalam situs internet dapat dicari apa saja tentang pornografi, dan ini akan memengaruhi orang-orang yang mengaksesnya. Apabila kemudian diaplikasi dalam kehidupan bermasyarakat, maka akan terjadi perbuatan asusila.

Pada bulan Mei 2003 Satuan Reskrimsus *cyber crime* Polda Metro Jaya menangkap mucikari *cyber*. Pelakunya sepasang suami istri, Ramdoni alias Rino dan Yanti Sari alias Bela. Prostitusi *cyber* ini adalah modus baru, menawarkan berbagai wanita melalui sebuah alamat *web*.

Dalam *web* tersebut ditampilkan deretan foto wanita dalam bentuk *close up* atau dalam busana minim yang siap melayani pria. Pengelola situs terlihat tidak

²⁴*Ibid.*, h. 65.

malu-malu menampilkan nomor telepon genggamnya, sehingga para peminat bisa memesan wanita yang dikehendaki, lalu pesanan tersebut diantar ke hotel atau apartemen sesuai pesanan.²⁵

3. *Hacker*

Hacker adalah orang yang memasuki atau mengakses jaringan komputer secara tidak sah (tanpa izin) dengan suatu alat dan program tertentu, bertujuan untuk merusak, merubah data dengan menambah atau mengurangi. Kejahatan yang dilakukan *hacker* berdampak terhadap kerusakan jaringan komputer, tetapi unsur-unsur kejahatan dimaksud belum terjangkau oleh undang-undang. Kalau kejahatan konvensional, seperti memasuki pekarangan orang lain tanpa izin sudah jelas aturannya sebagaimana yang tertuang dalam Pasal 167 KUHP.²⁶

Kalau *hacker* memasuki jaringan komputer tidak secara fisik, melainkan menggunakan alat dengan program tertentu. Dengan sistem hukum yang berlaku di Indonesia alat bukti elektronik seperti belum diatur, oleh karena itu diperlukan perangkat hukum khusus *cyber crime*.

Di samping hal tersebut, perlu dipahami bahwa para *hacker* dapat digolongkan menjadi 2 (dua) kelompok yaitu, *white hat hacker* dan *black hat hacker*, sebagaimana diungkapkan oleh Imam Syahputra. Dengan mengacu pada tulisan Steven Furnell, Imam Syahputra menyatakan bahwa:

Kelompok ‘putih’ atau *white hat hacker*, cenderung memiliki misi seperti ‘Robin Hood’. Mereka berusaha untuk menghambat atau memperbaiki suatu sistem komputer yang telah dirusak. Hal itu sebabnya, kelompok ini sering disebut sebagai *Cyber Warriors* atau *Samurai*. Sedangkan untuk para *hacker*,

²⁵*Ibid.*, h. 67.

²⁶*Ibid.*, h. 68.

hactivis, *malware writers* dan *cracker* digolongkan sebagai *black hat hacker*. Mereka ini lebih pada sifat merusak dan mengganggu orang lain.²⁷

Sejalan dengan hal tersebut, Sutanto dan kawan-kawan menyatakan, bahwa orang-orang yang melakukan kejahatan maya (*cyber crime*) pada umumnya dikenal sebagai *cracker* dan *hacker*. Dengan demikian, pelaku *cyber crime* dapat digolongkan menjadi 2 (dua) kelompok, yaitu *cracker* dan *hacker*.²⁸

Lebih lanjut Sutanto dan kawan-kawan menyatakan bahwa *cracker* adalah seseorang yang melakukan tindakan kejahatan dengan memasuki serta mengganggu hingga merusak sistem orang lain. Sedangkan tindakan seorang *hacker* tidak sampai merusak, yang dilakukan biasanya hanya sekedar mengintip informasi tentunya secara diam-diam, tanpa melakukan perubahan apapun terhadap sistem yang dia masuki.²⁹

Perbuatan para *black hat hacker* dan *cracker* tentu menimbulkan berbagai masalah. Perbuatan mereka dapat merugikan orang lain secara finansial, merusak sendi-sendi perekonomian hingga stabilitas keamanan suatu negara.

4. Merusak situs milik negara

Jenis kejahatan ini dinilai sangat merugikan negara, karena di samping data-data penting, dokumen rahasia negara dapat terbongkar yang akan mengancam eksistensi negara. Hal ini pernah terjadi pada kasus pembobolan situs KPU tahun 2004 yang dilakukan oleh Tersangka Dani Firmansyah pada situs KPU, <http://tnp.kpu.go.id> yang dilakukan pada tanggal 17 April 2004, dengan mengubah

²⁷Imam Syahputra, *Problematika Hukum Internet Indonesia* (Jakarta: Prenhallindo, 2002), h. 146.

²⁸Sutanto, Hermawan Sulistiyo, dan Tjuk Sugiarto, *Cyber Crime - Motif dan Penindakan* (Jakarta: Pensil 324, 2005), h. 15.

²⁹*Ibid.* h. 15.

tampilan beberapa nama partai menjadi nama lain, menyerang *server* KPU tersebut di atas dengan cara *Structured Query Language (SQL) Injection* (menyerang dengan cara memberi perintah melalui program SQL) dan berhasil menembus situs KPU, tnp.kpu.go.id 203.130.201.134 serta berhasil *up date* tabel nama partai menjadi nama lain yang tidak dikenal masyarakat, yang mengakibatkan terjadinya gangguan fisik elektromagnetik, dilakukan dengan cara *hacking* dari IP 202.158.10.117 di PT Danareksa kemudian membuka IP Proxy Anonymous Thailand 208.147.1.1 dengan maksud *spoofing* (penyesatan).³⁰

Kejadian-kejadian sebagaimana hal tersebut tentu meresahkan semua pihak. Oleh karena itu, jika tidak ditangani dengan cepat, maka akan merugikan negara dan masyarakat.

Selain beberapa jenis-jenis *cyber crime* yang dipaparkan tersebut, masih banyak jenis-jenis *cyber crime* yang lainnya, seperti yang diungkapkan oleh Didik M. Arief Mansur dan Alisatris Gultom yang menyatakan bahwa jenis-jenis kejahatan yang masuk dalam kategori *cyber crime* di antaranya:

1. *Cyber Terrorism*
2. *Cyber Pornography*
3. *Cyber Harassment*
4. *Cyber Stalking: crimes of stalking*
5. *Hacking*
6. *Carding (credit card fraud)*.³¹

³⁰Sutarman, *op. cit.*, h. 71.

³¹Didik M. Arief Mansur dan Alisatris Gultom, *Cyber Law – Aspek Hukum Teknologi Informasi* (Bandung: Refika Aditama, 2005), h. 26.

Sementara itu, menurut Sutanto dan kawan-kawan, secara garis besar *cyber crime* terdiri dari 2 (dua) jenis, yaitu:

1. Kejahatan yang menggunakan Teknologi Informasi (TI) sebagai fasilitas.

Adapun contoh-contoh dari aktivitas *cyber crime* jenis ini adalah pembajakan (*copyright* atau hak cipta intelektual); pornografi; pemalsuan dan pencurian kartu kredit (*carding*); penipuan lewat *e-mail*; penipuan dan pembobolan rekening bank; perjudian *on line*; terorisme; situs sesat; materi-materi internet yang berkaitan dengan isu suku, agama, ras dan antar golongan (SARA) seperti menyebarkan kebencian etnik, ras dan agama; transaksi dan penyebaran obat terlarang; transaksi seks; dan lain-lain.

2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran.

Cyber crime jenis ini bukan memanfaatkan komputer dan internet sebagai media atau sarana tindak pidana, akan tetapi menjadikannya sebagai obyek sasaran. Contoh dari jenis-jenis tindak kejahatannya antara lain pengaksesan ke suatu sistem secara ilegal (*hacking*), perusakan situs internet dan *server* data (*cracking*), serta *defacting*.³²

Dengan mengacu pendapat Nazura Abdul Manap, *cyber crime* dapat dibedakan ke dalam 3 (tiga) kelompok kategori, yaitu: *pertama*, *cyber crimes against property* (kejahatan maya terhadap hak milik). Misalnya, pencurian informasi properti, dan pelayanan, *fraud* atau *cheating*, *forgery*, dan *mischief*. Tiga yang terakhir menyangkut perilaku penipuan, pemaksaan, penjangbretan, dan yang semacam.

³²Sutanto, Hermawan Sulistiyo, dan Tjuk Sugiarto, *op. cit.*, h. 21.

Kedua, cyber crimes against Persons (kejahatan maya terhadap orang). Kejahatan ini meliputi pornografi, *cyber harassment* (pelecehan, seperti pelecehan seksual, terhadap seseorang melalui dunia maya), *cyber stalking* (mengejar-ngejar seseorang atau mengikuti terus-menerus sehingga mengganggu orang yang dikejar-kejar), dan *cyber trespass* ini dibagi lagi ke dalam *spam e-mail*, *web hacking*, dan *breaking to PC*. Intinya, masuk ke dalam wilayah pribadi seseorang tanpa izin.

Ketiga, adalah cyber terrorism. Terorisme maya (*cyber terrorism*) berdimensi luas, tetapi semua menyangkut isu-isu terorisme, mulai dari sekadar pemanfaatan jasa internet untuk berkomunikasi melakukan tindak kejahatan terorisme, hingga pemanfaatan langsung jaringan maya untuk melakukan teror publik.³³

Sedangkan menurut Abdul Wahid dan Mohammad Labib, pembagian jenis *cyber crime* ada 2 (dua) jenis, yaitu: kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas dan kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran. Menurut mereka, contoh jenis pertama adalah *credit card fraud*, *banking fraud*, *pornografi*, dan peredaran obat terlarang melalui internet. Sedangkan *defecting* dan *hacking* bisa digolongkan pada jenis kedua. Dalam kasus jenis pertama ini, kedudukan internet sebagai media teknologi informasi sebagai media teknologi canggih telah disalahfungsikan sebagai alat kriminalitas yang tidak hanya membahayakan masyarakat regional, tetapi juga masyarakat global.³⁴

³³Sebagaimana dikutip oleh Sutanto Hermawan Sulistiyo, dan Tjuk Sugiarto (Ed). Lihat dalam: *Ibid*, h. 14.

³⁴Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, (Jakarta: Refika Aditama, [t.th]), h. 131.

Menurut NCIS Inggris, sebagaimana dikutip oleh Ade Maman Suherman, menyatakan bahwa manifestasi dari tindak pidana *cyber crime* muncul dalam berbagai macam atau varian sebagai berikut:

1. *Recreational Hackers*

Kejahatan ini dilakukan oleh *netter* tingkat pemula untuk sekadar mencoba kekuranghandalan sistem sekuritas suatu perusahaan.

2. *Crackers* atau *criminal minded hackers*

Pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase, dan penghancuran data. Sebagai contoh, pada tahun 1994 Citibank AS kebobolan senilai 400.000 dolar oleh *cracker* dari Rusia yang akhirnya dijatuhi hukuman penjara selama tiga tahun serta harus mengembalikan sejumlah uang tersebut. Tipe kejahatan ini dapat terjadi dengan bantuan orang dalam, biasanya staf yang sakit hati atau datang dari kompetitor dalam bisnis sejenis.

3. *Political Hackers*

Aktivitas politik atau lebih populer dengan sebutan *hactivist* melakukan perusakan terhadap ratusan *situs web* untuk mengkampanyekan program-programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendeskreditkan lawannya. Usaha tersebut pernah dilakukan secara aktif dan konsisten dalam usaha untuk kampanye anti – Indonesia dalam masalah Timor Timor yang dipelopori oleh Ramos Horta. Situs Deplu (departemen luar negeri) sempat mendapat serangan yang diduga keras dari kelompok anti integrasi.

4. *Denial of Service Attack*

Serangan *denial of service attack* atau oleh FBI dikenal dengan istilah “*unprecedented*” tujuannya adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna yang *legitimate*. Taktik yang digunakan adalah dengan mengirim atau membanjiri *situs web* dengan data yang tidak perlu. Pemilik *situs web* menderita kerugian karena untuk mengendalikan atau mengontrol kembali situs web memakan waktu yang tidak sedikit.

5. *Insiders* atau *Internal Hackers*

Insider hackers ini bisa dilakukan oleh orang dalam perusahaan sendiri. Modus operandinya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan. Departemen Perdagangan dan Industri Inggris mengumumkan bahwa pada tahun 1998 ada banyak perusahaan-perusahaan yang telah menderita kerugian senilai 1,5 miliar poundsterling.

6. *Viruses*

Program pengganggu (*malicious*) dengan penyebaran virus dewasa ini dapat menular melalui aplikasi internet. Sebelumnya, pola penularan virus hanya melalui *floppy disk*. Virus bisa bersembunyi dalam file dan ter-*down load* oleh *user* bahkan bisa menyebar melalui kiriman *e-mail*. Seperti halnya dunia kedokteran, dunia komputer telah menciptakan jurus antivirus, seperti *melissa* 1999 atau *lovebug* 2000, tetapi masih belum bisa berbuat banyak.

7. *Piracy*

Pembajakan *software* merupakan *trend* dewasa ini. Pihak produsen *software* dapat kehilangan profit karena karyanya dapat dibajak melalui *down load* dari

internet dan di kopi ke dalam CD-Rom yang selanjutnya diperbanyak secara ilegal atau tanpa seizin penciptanya.

8. *Fraud*

Fraud adalah sejenis manipulasi informasi keuangan dengan tujuan mengeruk keuntungan sebesar-besarnya. Sebagai contoh, harga tukar saham yang menyesatkan melalui rumor. Situs lelang fiktif dengan mengeruk uang masuk dari para peserta lelang dan barangnya tidak dikirim bahkan identitas pelakunya tidak dapat dilacak.

9. *Gambling*

Perjudian di dunia saiber yang berskala global sulit dijerat dengan hukum nasional suatu negara. Dari kegiatan gambling dapat diputar kembali di negara yang merupakan *tax heaven*, seperti *Cayman Island* yang merupakan surga bagi *money laundering*. Bahkan Indonesia negara yang sering dijadikan sebagai tujuan *money laundering* yang uangnya diperoleh dari hasil kejahatan berskala internasional.

10. *Pornography and Paeddophilia*

Dunia *cyber* selain mendatangkan berbagai kemudahan dengan mengatasi kendala ruang dan waktu, juga telah melahirkan dunia pornografi yang mengkhawatirkan berbagai kalangan. Melalui *news group*, *chat rooms* mengeksploitasi pornografi anak-anak di bawah umur.

11. *Cyber - Stalking*

Cyber - Stalking adalah segala bentuk kiriman *e-mail* yang tidak dikehendaki oleh *user* atau *junk e-mail* yang sering memadati *folder* serta tidak jarang dengan pemaksaan meskipun *e-mail* "sampah" tidak dikehendaki oleh *user*. Bahkan sering juga pelaku/pengirim secara paksa memperoleh identitas personal secara detail calon para korbannya.

12. *Hate Sites*

Situs ini sering dipergunakan untuk saling menyerang dan melontarkan komentar-komentar yang tidak sopan dan vulgar yang dikelola oleh para ekstrimis. Penyerangan terhadap lawan atau *opponent* sering mengangkat isu rasial, perang program dan promosi kebijakan atau suatu pandangan.

13. *Criminal Communications*

NCIS telah mendeteksi bahwa internet telah dijadikan sebagai alat handal dan modern untuk melakukan komunikasi antar gangster, anggota sindikat obat bius, dan komunikasi antar *hooligan* di dunia sepak bola.³⁵

Paparan tentang jenis *cyber crime* yang lain adalah sebagaimana yang dikemukakan oleh Ahmad M. Ramli dan kawan-kawannya. Adapun jenis-jenis kejahatan yang terjadi di dunia maya (*cuber crime*) menurut Ahmad M. Ramli dan kawan-kawannya adalah sebagai berikut:

Pertama, pelanggaran isi *situs web*. Jenis pelanggaran ini ada 2 (dua), yaitu:

- a. Pornografi; dan
- b. Pelanggaran Hak Cipta.

Kedua, pelanggaran dalam perdagangan secara elektronik (*e-commerce*).

Yang termasuk dalam pelanggaran ini adalah:

- a. Penipuan *on-line*;
- b. Penipuan pemasaran berjenjang *on line*; dan
- c. Penipuan kartu kredit.

Ketiga, pelanggaran lainnya, seperti:

³⁵NCIS Inggris dalam Ade Maman Suherman, *Aspek Hukum Dalam Ekonomi Global* (Jakarta: Ghalia Indonesia, 2002), h.168-171.

- a. *Recreational hacker*;
- b. *Cracker atau criminal minded hacker*;
- c. *Political hacker*;
- d. *Denial of Service Attack (DoS)*;
- e. *Viruses*;
- f. *Pembajakan (Piracy)*;
- g. *Fraud*;
- h. *Phising*;
- i. *Perjudian (Gambling)*; dan
- j. *Cyber Stalking*.³⁶

Sedangkan menurut Ari Juliano Gema, sebagaimana dikutip oleh Abdul Wahid dan Mohammad Labib, menyatakan bahwa *cyber crime* dapat dikelompokkan dalam beberapa bentuk, yaitu:

1. *Unauthorized Acces to Computer System and Service*. Kejahatan ini dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik jaringan komputer yang dimasukinya. Motifnya bisa bermacam-macam, antara lain adalah sabotase, pencurian data dsb. Contoh adalah *website* pemerintah RI dirusak oleh *hacker*.

2. *Illegal Contents*. Kejahatan ini dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu yang tidak benar, tidak etis, dan dapat melanggar hukum atau mengganggu ketertiban umum. Contoh yang termasuk kejahatan jenis ini adalah pornografi, pemuatan berita bohong, agitasi termasuk juga

³⁶Ahmad M. Ramli, Pager Gunung dan Indra Apriadi, *Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik* (Jakarta: Departemen Komunikasi dan Informatika RI, 2005), h. 62-66.

delik politik dapat dimasukkan kategori ini bila menggunakan media ruang saiber (*cyber*).

3. *Data Forgery*. Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.

4. *Cyber Espionage*. Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau datanya tersimpan dalam suatu sistem yang *computerized*.

5. *Cyber Sabotage and Extortion*. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program tertentu sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Kejahatan ini juga kadang disebut dengan *cyber terrorism*.

6. *Offence Againsts Intellectual Property*. Kejahatan ini ditujukan terhadap HaKI yang dimiliki pihak lain di internet. Sebagai contoh, meniru tampilan *web* suatu situs tertentu, penyiaran rahasia dagang yang merupakan rahasia dagang orang lain.

7. *Infringements of Privacy*. Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan secara *computerized*. Yang apabila diketahui oleh orang lain, maka dapat merugikan

korban secara material atau immaterial, seperti PIN ATM, nomor kartu kredit dan sebagainya.³⁷

Sejalan dengan perkembangan teknologi informasi maka kiranya dapat disimpulkan bahwa berbagai jenis baru atau “*spesies*” baru dari kejahatan dunia maya (*cyber crime*) akan terus bermunculan. Setiap orang akan menjadi semakin gelisah dengan perkembangan kejahatan di dunia maya. Oleh karena itu, pemerintah perlu melakukan upaya-upaya preventif maupun represif dalam menanggulangi kasus-kasus kejahatan di dunia maya tersebut.

C. Sejarah Cyber Crime

Cyber crime merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional (*street crime*). *Cyber crime* muncul bersamaan dengan lahirnya revolusi teknologi informasi. sebagaimana dikemukakan oleh Ronni R. Nitibaskara bahwa:

Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi seperti ini, penyimpangan hubungan sosial yang berupa kejahatan (*crime*), akan menyesuaikan bentuknya dengan karakter baru tersebut.³⁸

Ringkasnya, sesuai dengan ungkapan: “kejahatan merupakan produk dari masyarakatnya sendiri” (*crime is a product of society it's self*), “habitat” baru ini, dengan segala bentuk pola interaksi yang ada di dalamnya, akan menghasilkan jenis-jenis kejahatan yang berbeda dengan kejahatan-kejahatan lain yang sebelumnya

³⁷ Abdul Wahid dan Mohammad Labib, *op. cit.*, h. 72-73.

³⁸ Lihat Dikdik M. Arief Mansur dan Alisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi* (Bandung: PT Refika Aditama, 2005), h. 25 dalam Tubagus Ronny Rahman Nitibaskara, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Krimonologi Hukum dan Sosiologi* (Jakarta: Peradaban, 2001), h. 38.

telah dikenal. Kejahatan-kejahatan ini berada dalam satu kelompok besar yang dikenal dengan istilah *cyber crime*.³⁹

Selanjutnya akan ditelusuri dan dikaji mengenai munculnya *cyber crime* di Indonesia. Dari referensi yang ada di Indonesia menunjukkan bahwa munculnya *cyber crime* pertama kali di Indonesia tidak dapat ditelusuri kejadiannya, kapan, dan dalam kasus apa. Namun demikian, dapat dikemukakan bahwa era 1990-an adalah era awal masuknya fenomena *cyber crime* di Indonesia.

Dilihat dari putusan pengadilan, ada yang menyatakan, bahwa kasus yang pertama kalinya disidangkan di Indonesia adalah kasus pemakaian nama domain mustikaratu.com di Pengadilan Negeri Jakarta Selatan. Perkara ini menyeret seorang terdakwa bernama Tjandra Sugijono dengan dakwaan Pasal 382 bis KUHP dan Pasal 48 ayat (1) jo. Pasal 19 huruf b UU No. 5 tahun 1999 tentang Larangan Praktik Monopoli dan Persaingan Usaha Tidak Sehat. Dalam pemeriksaan tersebut, majelis hakim Pengadilan Negeri Jakarta Selatan memutuskan bahwa perbuatan yang didakwakan tersebut tidak terbukti, sehingga Tjandra Sugijono dibebaskan dari segala dakwaan (*vrijspraak*).⁴⁰

Di samping hal tersebut, kasus yang muncul kepermukaan dan diketahui oleh publik pada umumnya adalah berdasarkan laporan tertangkapnya para pelaku *cyber crime* atau laporan dari korban *cyber crime* dengan kerugian yang dialaminya.

³⁹*Ibid.*

⁴⁰Dalam bukunya Sutarman, *Cyber Crime: Modus Operandi dan Penanggulangannya* pada halaman 7 disebutkan dalam kutipannya bahwa, berdasarkan Salinan Putusan Pengadilan Negeri Jakarta Selatan yang dibacakan pada hari Selasa tanggal 11 Desember 2001 dengan Ketua Majelis Hakim Ny. Chasiah R. Tandjung, SH., dan Anggota Majelis Hakim masing-masing Musa Simatupang, SH., dan Ali Kamal Haky, SH.

Berikut ini adalah fakta-fakta yang mencerminkan kemunculan *cyber crime* di Indonesia.

Di Bandung misalnya, banyak Warung Internet (warnet) yang menjadi sarang *cyber crime*. Tidak dapat disangkal, Bandung merupakan salah satu kota tertinggi kedua *cyber crime* setelah Yogyakarta. Warnet di Bandung yang terdaftar di Awari mencapai 400-an dari total 600-an warnet. Selebihnya tidak menjadi anggota asosiasi karena memang tidak ada ketentuan yang mengharuskan mereka bergabung dalam wadah asosiasi. Bahkan, ketua asosiasi warnet Bandung pernah menjadi korban *cyber crime* karena warnetnya dipakai pelanggan untuk *carding* (kejahatan internet dengan membobol kartu kredit orang lain untuk bertransaksi).⁴¹

Contoh yang lain pernah terjadi di Yogyakarta. Dalam kasus tersebut, seorang pemuda berusia 22 tahun bernama Petrus Pangkur bersama 3 (tiga) orang rekannya sesama *cracker* berhasil membobol lewat internet. Pada akhirnya mereka ditangkap oleh Kepolisian Yogyakarta dengan tuduhan membeli barang melalui internet dengan cara tidak sah. Pada bulan Maret dan April 2001 mereka berhasil membobol kartu kredit orang lain sebesar Rp. 5 Milyar. Kasus pembobolan ini terungkap setelah ada surat dari Departemen Luar Negeri dan Kepolisian Internasional. Menurut surat itu, ada nama-nama pembeli barang dari luar negeri dengan kartu kredit lewat internet. Tetapi setelah barang dikirim, kartu kredit tidak diakui oleh pemiliknya. Kemudian, para pelaku dapat ditangkap setelah polisi melakukan pelacakan ke beberapa perusahaan jasa angkutan di Yogyakarta.⁴²

⁴¹Abdul Wahid dan Mohammad Labib, *op. cit.*, h. 127-128.

⁴²Dikdik M. Arief Mansur dan Alisatris Gultom, *op. cit.*, h. 11.

Di Semarang juga pernah terjadi kasus yang hampir sama dengan kasus di Yogyakarta. Kepolisian Wilayah Semarang berhasil menangkap 2 (dua) orang pemuda pada saat mereka akan mengambil pesanan barang di sebuah jasa pengiriman. Barang yang akan diambil adalah 8 (delapan) buah kacamata, 4 (empat) topi, dan 3 (tiga) tas punggung merek *Oakley* seharga Rp. 8 juta. Akan tetapi, mereka tidak mampu menunjukkan kartu kredit yang sah. Pada akhirnya mereka ditangkap polisi.⁴³

Di tengah kemajuan dalam bidang teknologi informasi yang dilakukan negara-negara tetangga, kondisi negeri ini memang cukup memprihatinkan. Dari data yang ada menunjukkan bahwa negara yang masuk kelompok lima besar pengguna internet di dunia adalah Amerika Serikat, Jepang, China, Inggris dan Jerman. Menurut Sutanto dan kawan-kawan, yang menarik dari kelima negara itu adalah negara China. Sekalipun China tidak atau belum termasuk sebagai negara maju dan secara resmi masih merupakan negara komunis, ternyata telah tercatat sebagai negara peringkat ke tiga dalam hal penggunaan internet.⁴⁴

Melihat kenyataan ini dipastikan *cyber crime* akan terus berkembang pesat seiring dengan berkembangpesatnya teknologi informasi (TI).

D. Ruang Lingkup Cyber Crime

Dalam melihat ruang lingkup *cyber crime* harus didasarkan pada undang-undang yang mengaturnya. Undang-undang yang dimaksud adalah Undang-Undang

⁴³*Ibid.*

⁴⁴Sutanto, Hermawan Sulistiyo, dan Tjuk Sugiarto, *op. cit.*, h. 11.

Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Dalam undang-undang tersebut pada Pasal 1 ayat (2) disebutkan bahwa:

Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.⁴⁵

Merujuk dari pasal tersebut, dapat dipahami bahwa transaksi elektronik sebagai suatu perbuatan hukum yang dilakukan dengan komputer dan jaringan komputer, dapat juga dilakukan melalui sarana/media elektronik lainnya, seperti *lap top* dan *hand phone*.⁴⁶

Berkaitan dengan hal tersebut, untuk mengetahui lebih lanjut tentang ruang lingkup *cyber crime* dapat juga dilihat melalui pengertian *cyber crime* sebagai berikut:

Pada pembahasan sebelumnya disebutkan bahwa, *Cyber crime* adalah kejahatan yang muncul sebagai dampak negatif dari perkembangan aplikasi internet.⁴⁷ Pengertian ini membatasi pada ruang aplikasi internet, sehingga jika pelaku menggunakan LAN (*local area network*), maka akan lepas dari target hukum. Karena hanya dibatasi oleh sarana internet meskipun sama-sama menggunakan media komputer. Oleh karena itu, definisi tersebut tidak menyebutkan media elektronik tertentu, tetapi memfokuskan pada dampak aplikasi internet.

⁴⁵Redaksi New Merah Putih, *Undang-Undang ITE (Informasi dan Transaksi Elektronik)* (Cet. I; Yogyakarta: New Merah Putih, 2009), h. 11.

⁴⁶*Hand phone* akhir-akhir ini marak digunakan oleh pengguna internet sebagai sarana transaksi melalui internet selain digunakan sebagai alat komunikasi. Sehingga seorang pelaku kejahatan dunia maya (*cyber crime*) tidak perlu mendatangi layanan warung internet (WARNET) atau kios internet (KIOSNET), tetapi cukup di kamar ukuran 2x3 meter dengan leluasa melakukan kejahatan tersebut.

⁴⁷<http://www.thecelia.com/dokumen/jurnal/ajo.a002.shtml>. (Diakses pada tanggal 25 Juni 2010)

Sedangkan menurut Kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.⁴⁸

Pengertian tersebut menarik, karena pengertian ini memiliki kesamaan dengan Undang-Undang ITE, yakni menggunakan jaringan komputer. Dari 2 (dua) definisi tersebut yang menjadi catatan adalah bahwa dalam definisi tersebut tidak dijelaskan apa maksud kata “jaringan komputer”. Apabila dimaknai secara luas maka akan meliputi LAN (*local area networking*) dan internet. LAN ini mempunyai karakter yang berbeda dengan internet. LAN merupakan jaringan tertutup. Dalam beberapa segi, jenis kejahatan yang disebut termasuk dalam katagori *cyber crime* tidak dapat dilakukan dalam LAN ini, seperti *spamming*, *cybersquatting*.

Dengan demikian media elektronik apapun yang dapat digunakan sebagai sarana teraksesnya internet dan transaksi elektronik merupakan bagian yang dimaksudkan oleh Undang-Undang ITE. Sehingga, siapapun sebagaimana dimaksud dalam undang-undang yang melakukan kejahatan dalam ruang dan batas sebagaimana dijelaskan, maka di kategorikan sebagai tindak kejahatan mayantara (*cyber crime*).

Oleh karena itu, menjadi terbedakan antara tindak pidana *cyber crime* dan konvensional. Dalam *cyber crime* tidak terjadi kontak fisik antara subyek dan obyek melainkan melalui media elektronik. Sedangkan kejahatan konvensional melalui kontak fisik secara langsung yang dengan mudah diketahui pelakunya atau subyeknya.

⁴⁸Lihat Abdul Wahid dan Mohammad Labib, *op. cit.*, h. 40.

BAB III

KONSEPSI *CYBER CRIME* DALAM HUKUM PIDANA DI INDONESIA

A. Hakikat Cyber Crime dan Eksistensinya dalam Undang-Undang ITE

Cyber crime adalah suatu istilah yang digunakan oleh para ahli hukum khususnya hukum siber (*cyber law*).¹ Hal ini dapat dilihat dalam pembahasan pada bab sebelumnya (bab ii).

Sejalan dengan hal tersebut, *cyber crime* pada prinsipnya adalah tindakan yang dilakukan oleh pelaku kejahatan yang memanfaatkan perkembangan teknologi informasi. Hal ini juga menunjukkan bahwa *cyber crime* merupakan bagian dari sisi-sisi dan realitas yang tidak terpisahkan dari teknologi informasi itu sendiri.

Sutanto dan kawan-kawan menyatakan, bahwa teknologi informasi semakin memegang peranan penting dalam kehidupan, dan telah membawa sejumlah manfaat, antara lain kemudahan memperoleh dan menyampaikan informasi serta iptek, meningkatkan transaksi perdagangan, bisnis dan bahkan untuk isu-isu yang sebelumnya sangat bersifat pribadi, seperti situs porno dan *chatting*. Akan tetapi, di samping segala kemudahan yang ditimbulkan, internet juga memunculkan potensi kejahatan baru yang disebut *cyber crime*. Lebih lanjut dinyatakan bahwa *cyber crime* adalah suatu kejahatan baru yang sangat berbeda dengan dua jenis kejahatan yang

¹Istilah “Hukum Siber” diartikan sebagai padanan kata dari “*Ciber Law*”, yang saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah Hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara. Penjelasan tersebut dapat dilihat dalam Ahmad M. Ramli, *Cyber Law dan HAKI-dalam Sistem Hukum Indonesia* (Cet. I; Bandung: PT Refika Aditama, 2004), h. 1.

sudah ada sebelumnya, *blue collar crime* (arti harfiahnya kejahatan kerah biru) dan *white collar crime* (arti harfiahnya kejahatan kerah putih).²

Blue collar crime adalah kejahatan konvensional seperti pencurian, pembunuhan dan lain-lain. Sedangkan *white collar crime*, menurut Jo Ann Miller, umumnya dibagi ke dalam 4 (empat) jenis, yaitu: kejahatan korporasi, kejahatan birokrasi, malpraktek dan kejahatan individu.³

Sementara itu, *cyber crime* memiliki ciri khas tersendiri. Para pelaku pada umumnya anak-anak muda yang menguasai teknologi informasi. Dalam berbagai kasus yang telah terungkap dan pelakunya tertangkap, sebagian di antaranya terbukti bahwa pelakunya adalah anak-anak muda, bahkan masih remaja. Di antara kasus-kasus besar tersebut, ada di antaranya yang merupakan hasil dari sekedar tindakan “iseng” atau coba-coba”.⁴

Sebagai perbandingan dari hal tersebut, Ahmad M. Ramli menyatakan, teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif untuk melakukan perbuatan melawan hukum.⁵

Pernyataan Ahmad M. Ramli di atas menjadi alasan pembenaran terhadap suatu adagium “di mana ada masyarakat, di situ ada kejahatan”.⁶ Dua sisi inilah yang menjadi realitas potret kehidupan yang sebenarnya. Konsep yang dibangun

²Sutantu, Hermawan Sulistiyo dan Tjuk Sugiarto dalam Sutarman, *Cyber Crime: Modus Operandi dan Penanggulangannya* (Cet. I; Yogyakarta: LaksBang Pressindo, 2007), h. 31.

³*Ibid.*, h. 31-32.

⁴*Ibid.*

⁵Achmad Sodiki dalam Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Cet. I; Bandung: Refika Aditama, 2005), h. vii.

⁶*Ibid.*

secara ideal selalu melahirkan realitas lain yang menyimpang dari konsep ideal tersebut, yakni tindakan melawan hukum (kejahatan dan pelanggaran).

Adagium lain seperti “*ubi societis, ibi ius*” (di mana ada masyarakat di situ ada hukum) juga ikut membenarkan, bahwa kriminalitas yang terjadi sejatinya adalah cermin riil kehidupan masyarakat, bahwa ada tali-temali antara hukum masyarakat, dan kriminalitas. Masyarakat membutuhkan hukum, karena masyarakat mencita-citakan kehidupan yang damai, tertib, nyaman atau agar hak-haknya tidak diganggu oleh yang lain. Demikian itu merupakan terjemahan dari kepentingan fundamental masyarakat yang sebenarnya menempatkan antara kejahatan dengan hukum dalam posisi *vis a vis* (saling berlawanan)⁷.

Selanjutnya dikemukakan bahwa munculnya *cyber crime* merupakan suatu pembenaran bahwa era global ini identik dengan era ranjau ganas. Sebuah ruang imajiner dan maya, area atau zona bagi setiap orang untuk melakukan aktivitas yang bisa dilakukan dalam kehidupan sosial sehari-hari dengan cara artifisial. Setiap orang bisa saling berkomunikasi, menikmati hiburan, dan mengakses apa saja yang menurutnya bisa mendatangkan kesenangan atau kepuasan. Ada beragam tawaran di ruang maya sesuai informasi global yang dijual oleh kapitalis-kapitalis yang rela menghalalkan segala cara untuk mendapatkan keuntungan. Bahkan ironisnya, mereka juga bermaksud meruntuhkan ketahanan moral, ideologi dan agama-agama bangsa lain di muka bumi yang berbeda dengan dirinya.⁸

Realitas tersebut menunjukkan secara nyata, bahwa peradaban dunia tidak stagnan. Peradaban dunia terlihat sangat dinamis karena perkembangan pola pikir

⁷*Ibid.*

⁸Sutarman, *op. cit.*, h. 29.

dan kemajuan teknologi yang sangat pesat. Dinamisasi kehidupan dunia ini memicu perubahan terhadap ideologi, sosial, politik, ekonomi, dan pertahanan untuk mencapai suatu negara yang dicita-citakan. Di samping itu era perubahan terus dikembangkan baik pada lini sosial maupun iptek. Hal ini juga yang menjadi perbedaan dari perubahan suatu zaman, yakni zaman teknologi dan informasi.

Berkaitan dengan hal tersebut di atas, Alvin Toffler membagi era di dunia ini dalam tiga gelombang, yaitu: *Pertama*, gelombang pertama. Pada tahap ini manusia lebih cenderung mengembangkan ilmu pengetahuan dan teknologinya pada bidang pertanian. Sehingga sekitar tahun 8000 SM, muncul pengetahuan tentang teknologi bercocok tanam. Manusia kala itu (baca: pada saat itu) lebih senang tinggal di satu tempat yang kemudian menjadi manusia pedesaan. *Kedua*, gelombang kedua. Pada tahap ini manusia melalui sebuah revolusi besar yang terjadi di akhir abad ke 18 M. Ditandai dengan Revolusi Prancis yang melahirkan konsep demokrasi dengan semboyannya kebebasan, persamaan, dan persaudaraan. Persoalan-persoalan yang terjadi pada gelombang pertama, seperti dominasi, pemusnahan peradaban kelompok etnik yang kurang maju, penjajahan, beserta zaman imperialisme dapat diperbaiki. Di samping itu dengan adanya revolusi industri, manusia pada era ini sudah dapat memisahkan antara kegiatan produksi dan konsumsi. *Ketiga*, gelombang ketiga. Pada tahapan ketiga ini ditandai dengan lahirnya revolusi digital. Revolusi ini hasil penemuan-penemuan di bidang teknologi komunikasi dan informasi. Toffler menyebut masyarakat yang ada pada gelombang ketiga ini disebut sebagai masyarakat informasi.⁹

⁹Budi Agus Riswandi, *Hukum Cyberspace* (Cet. I; Yogyakarta: Gitanagari, 2006), h. 4. Baca juga Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: Rajawali Press, 2003).

Pendapat Toffler tersebut dipertegas oleh Budi Agus Riswandi dalam bukunya *Hukum Cyber Space*, Budi menjelaskan, di era digital ini sarana teknologi sangat memiliki peranan yang sangat vital, terutama teknologi yang berkaitan dengan penyebaran informasi. Teknologi seperti ini acapkali disebut teknologi informasi. Teknologi informasi sendiri memiliki pengertian sebagai suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, dan menyebarkan informasi.¹⁰

Demikian juga dengan realitas perkembangan teknologi informasi, *cyber crime* hadir menjadi sebuah eksistensi negatif dan membahayakan bagi perkembangan itu sendiri, karena kehadirannya tidak dikehendaki. Namun demikian, hal itu tidak dapat dinafikan karena sudah menjadi bagian dari sisi mata uang. Menafikan *cyber crime*, berarti menafikan terhadap perkembangan teknologi informasi. Hal ini cukup beralasan dengan adanya adagium di atas, “di mana ada masyarakat, di situ ada kejahatan”.

Hal pokok terpenting adalah bagaimana kejahatan itu bisa diminimalisir. Oleh karena itu, aturan hukum dapat tampil dan berperan menjadi panglima dalam memberantas tindakan-tindakan melawan hukum. Dalam kajian yuridis terhadap Undang-Undang ITE, istilah *cyber crime* tidak akan dijumpai di dalam undang-undang tersebut, karen istilah *cyber crime* hadir sebagai sebuah istilah yang diatributkan pada pelaku kejahatan yang menggunakan sarana kecanggihan teknologi informasi (internet).

Dengan dikeluarkan dan diberlakukannya pengaturan Undang-Undang ITE, maka pengelolaan, penggunaan dan pemanfaatan informasi dan transaksi elektronik harus terus dikembangkan melalui infrastruktur hukum dan pengaturannya. Sehingga

¹⁰*Ibid.*, h. 4-5.

pemanfaatannya dapat dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama, sosial dan budaya masyarakat Indonesia, serta untuk menjaga, memelihara, dan memperkuat persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan demi kepentingan nasional.

Kasus-kasus *cyber crime* yang merupakan perkembangan dari *computer crime* apabila dilakukan sebelum lahirnya Undang-Undang ITE, maka bagi pelakunya didakwa dengan menggunakan kriteria peraturan hukum pidana konvensional. Perbuatan pidana yang digunakan untuk menjerat pelakunya tersebut adalah penipuan, kecurangan, pencurian, perusakan, dan lain-lainnya yang pada pokoknya dilakukan secara langsung oleh pelaku. Jika dilakukan dengan memanfaatkan sarana komputer (internet) saat sekarang telah dapat diterapkan dengan pasal-pasal yang terdapat dalam Undang-Undang ITE tercantum dalam Bab 7 untuk ‘Perbuatan yang Dilarang’ (Pasal 27-37) dan dalam Bab 11 untuk “Ketentuan Pidana” (Pasal 45-52).¹¹

Selanjutnya, akan dibanding serta dipersandingkan antara Undang-Undang ITE dengan KUHP dan undang-undang lain yang terkait, baik mengenai sistem pembuktian atau alat bukti elektroniknya maupun mengenai jenis serta ancaman pidananya.¹²

Dengan demikian posisi *cyber crime* dalam Undang-Undang ITE menjadi terlihat jelas, karena undang-undang tersebut menjadi bagian integral dari rangkaian perundang-undangan yang mengaturnya. Sehingga *cyber crime* yang menjadi modus baru dalam kejahatan terhadap perkembangan teknologi informasi dapat

¹¹Ninie Suparni, *Cyber Space: Problematika dan Antisipasi Pengaturannya* (Cet. I; Jakarta: Sinar Grafika, 2009), h. 112-113.

¹²*Ibid.* h. 113.

ditanggulangi. Untuk itu, perundang-undang di Indonesia yang berkaitan dengan *cyber crime* harus terkonstruksi dengan sempurna agar kejahatan-kejahatan baru dapat terakomodir di dalamnya.

B. Faktor-Faktor yang Memengaruhi Terjadinya Cyber Crime

Era kemajuan teknologi informasi ditandai dengan meningkatnya penggunaan internet dalam setiap aspek kehidupan manusia. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, di sisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan tindak pidana. Menurut Didik M. Arief Mansur dan Elisatris Gultom, munculnya kejahatan dengan mempergunakan internet sebagai alat bantu (*cyber crime*) lebih banyak disebabkan oleh faktor keamanan pelaku dalam melakukan kejahatan, masih kurangnya aparat penegak hukum yang memiliki kemampuan dalam hal *cyber crime*.¹³

Berikut ini akan dipaparkan faktor-faktor yang memengaruhi terjadinya *cyber crime*. Faktor-faktor yang berpengaruh terhadap *cyber crime* ini difokuskan pada 3 (tiga) faktor, yaitu: faktor politik, faktor ekonomi dan faktor sosial budaya. Masing-masing akan dijelaskan berikut ini:¹⁴

1. Faktor Politik

Mencermati maraknya *cyber crime* yang terjadi di Indonesia dengan permasalahan yang dihadapi oleh aparat penegak, proses kriminalisasi di bidang *cyber* telah terjadi dan merugikan masyarakat. Media *cyber* memberitakan tentang

¹³Didik M. Arief Mansur dan Alisatris Gultom dalam Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya* (Cet. I; Yogyakarta: Laksbang Pressindo, 2007), h. 64.

¹⁴*Ibid.*

cyber crime yang dilakukan oleh orang Indonesia, sebagaimana kasus yang terjadi di Yogyakarta, dan beberapa kota lain mengakibatkan citra Indonesia kurang baik di mata dunia dalam penegakan hukum *cyber crime*.

Penyebaran virus komputer dapat merusak jaringan komputer yang digunakan oleh pemerintah, perbankan, pelaku usaha maupun perorangan yang dapat berdampak terhadap kekacauan dalam sistem jaringan. Dapat dipastikan apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari dapat menimbulkan kekacauan pembayaran maupun transaksi keuangan bagi nasabah.

Kondisi ini memerlukan kebijakan politik pemerintah Indonesia untuk menanggulangi *cyber crime* yang berkembang di Indonesia. Aparat penegak hukum telah berupaya keras untuk menindak setiap pelaku *cyber crime*, tetapi penegakan hukum tidak dapat berjalan maksimal sesuai harapan masyarakat karena perangkat hukum yang mengatur khusus tentang *cyber crime* belum memadai.

Untuk menghindari kerugian yang lebih besar akibat tindakan pelaku *cyber crime*, maka diperlukan kebijakan politik pemerintah Indonesia untuk merevisi dan mempertajam perangkat hukum khusus (*lex specialist*) bagi *cyber crime*. Dengan perangkat hukum ini aparat penegak hukum tidak ragu-ragu lagi dalam melakukan penegakan hukum terhadap *cyber crime*.

2. Faktor Ekonomi

Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi. Jaringan komputer dan internet merupakan media yang sangat murah untuk promosi. Masyarakat dunia banyak yang memanfaatkan media ini untuk mencari barang-barang kepentingan perorangan maupun korporasi. Produk barang yang dihasilkan oleh industri di Indonesia sangat banyak dan digemari oleh

komunitas internasional, seperti barang-barang kerajinan, ukiran dan barang-barang lain. Para pelaku bisnis harus mampu memanfaatkan sarana internet dimaksud.

Krisis ekonomi yang melanda bangsa Indonesia harus dijadikan pelajaran bagi masyarakat Indonesia untuk segera bangkit dari krisis dimaksud. Seluruh komponen bangsa Indonesia harus berpartisipasi untuk mendukung pemulihan ekonomi. Media internet dan jaringan komputer merupakan salah satu media yang dapat dimanfaatkan oleh seluruh masyarakat untuk mempromosikan Indonesia.

Sehingga dengan kecanggihan teknologi informasi ini Indonesia mampu menjadi negara yang maju dan kuat, karena didukung oleh sumber daya manusia (SDM) yang siap dan mampu bersaing dengan negara-negara lainnya.

3. Faktor Sosial Budaya

Untuk faktor sosial budaya dapat dilihat dari beberapa aspek, yaitu:

a. Kemajuan Teknologi Informasi

Pesatnya kemajuan Teknologi Informasi tidak dapat dibendung oleh siapapun di negeri ini. Semua orang membutuhkan teknologi, informasi, bahkan 'levelitas' kebutuhan itu terhadap orang-orang tertentu yang maniak informasi dianggapnya sebagai sebuah kebutuhan primer, setelah kebutuhan makan dan minum. Sehari tanpa informasi, diibaratkan sehari tanpa minum, oleh karena itu, tidak mengherankan kemudian terbentuklah sebuah komunitas baru dunia teknologi informasi (TI) yang memainkan peranan penting bagi kesejahteraan manusia, termasuk pertumbuhan ekonomi, politik, budaya, dan aspek kehidupan yang lain.

Pada era globalisasi ini, manusia tidak akan bisa melepaskan kebutuhannya terhadap teknologi informasi. Dalam kehidupan sehari-hari manusia bergantung dengan teknologi informasi, mulai dari yang sederhana sampai dengan yang super

canggih. Yang sederhana seperti koran dan radio, namun keduanya ditunjang oleh teknologi yang canggih. Sedangkan yang canggih misalnya yang sehari-hari melekat pada tubuh manusia seperti *hand phone* dan *lap top* untuk membantu aktivitasnya.

Dengan teknologi informasi manusia dapat melakukan akses perkembangan lingkungan secara akurat, karena di situ ada kebebasan yang seimbang, bahkan dapat mengaktualisasikan dirinya agar dapat dikenali oleh lingkungannya. Menurut Agus Raharjo setidaknya ada 2 (dua) hal yang membuat teknologi informasi dianggap penting dalam memacu pertumbuhan ekonomi dunia:

- 1) Teknologi Informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya.
- 2) Memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya.¹⁵

Meskipun peranan tersebut lebih condong pada bidang ekonomi, namun dapat dilihat betapa pentingnya peranan teknologi informasi untuk mengefektifkan layanan dan kepentingan sebagai tenaga dorong kemajuan komunikasi global dengan berbagai pihak agar maksud dan tujuan masing-masing dapat tercapai.

b. Sumber Daya Manusia yang Mengawaki

Antara teknologi informasi dengan operator yang mengawaki mempunyai hubungan yang erat sekali, keduanya tidak dapat dipisahkan. Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali dari sebuah alat. Apakah alat itu digunakan sebagai sarana kebajikan untuk mencapai

¹⁵Agus Raharjo, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: Citra Aditya Bakti, 2002), h. 1.

kesejahteraan umat manusia, atautkah alat itu akan dikriminalisasikan sehingga dapat merusak kepentingan negara dan masyarakat.

teknologi sebagai hasil temuan dan pengembangan manusia kemudian dimanfaatkan, untuk perbaikan umat, namun di sisi lain dapat membawa petaka bagi umat manusia sebagai akibat adanya penyimpangan. Di Indonesia sumber daya pengelola teknologi informasi ini cukup, namun sumber daya manusia untuk memproduksi atau menciptakan teknologi ini masih kurang. Penyebabnya ada berbagai hal, di antaranya kurangnya tenaga peneliti dan kurangnya biaya penelitian atau mungkin kurangnya perhatian dan apresiasi terhadap penelitian. sehingga sumber daya manusia di Indonesia lebih banyak sebagai pengguna saja dan jumlahnya cukup banyak.¹⁶

c. Komunitas Baru

Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, di antaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologi terbentuklah sebuah komunitas baru di dunia maya yakni komunitas para pecandu internet yang saling berkomunikasi, bertukar pikiran berdasarkan prinsip kebebasan dan keseimbangan di antara para pecandu atau maniak dunia maya tersebut.

Komunitas ini adalah sebuah populasi gaya baru sebagai gejala sosial, dan sangat setrategis untuk diperhitungkan, sebab dari media ini banyak hikmah yang bisa didapat. Dari hal yng tidak tahu menjadi tahu, yang tahu jadi semakin pintar, sementara yang pintar semakin canggih. Terjadinya perkembangan teknologi dan

¹⁶Sutarman, *op. cit.* h. 88-89.

laju perkembangan masyarakat diketahui dengan cepat dan akurat, dan mereka saling bertukar pikiran serta dapat melakukan *rechecking* di antara mereka sendiri.

Secara emosional, mereka melekatkan dirinya kepada teman di dunia maya. salah satu bentuk komunitas itu adalah *mailing list*. Di yahoo terdapat komunitas dan kemudian difasilitasi oleh yahoo dalam bentuk group.yahoo.com. Dalam *mailing list* mereka dapat berdiskusi tentang suatu masalah, namun mereka tidak harus menghidupkan komputer dan internet secara bersamaan, sedangkan *chatting*, di antara mereka harus sama-sama menghidupkan komputer.¹⁷

d. Dampak *Cyber Crime* Terhadap Keamanan Negara

Setelah melihat beberapa faktor yang memengaruhi terjadinya *cyber crime*, uraian berikut ini akan membahas tentang dampak *cyber crime* terhadap keamanan negara yang dapat disorot dari aspek:

1) Kurangnya kepercayaan dunia terhadap Indonesia

Menurut Sutarman yang dikutip dari Budi Raharjo, Direktur Pusat Penelitian dan Pengembangan Industri dan Teknologi Informasi Institut Teknologi Bandung, di sejumlah kota besar seperti Bandung, Semarang, Yogyakarta, Surabaya, dan Jakarta, pelaku dan aksi *cyber crime* sebagian besar oknum terdidik seperti mahasiswa. Kejahatan macam ini terus berlangsung dalam tiga tahun belakangan ini.¹⁸

Hukuman terhadap pelaku cukup ringan, bahkan banyak pihak berpendapat, pelakunya adalah ‘pahlawan’ karena dapat membobol suatu situs dengan kemampuannya. Padahal, di balik kejahatan itu para pelaku telah menurunkan

¹⁷*Ibid.*, h. 90.

¹⁸*Ibid.*, h. 91.

derajat dan martabat bangsa Indonesia di mata dunia, karena merugikan pihak-pihak pebisnis melalui teknologi informasi atau dikenal praktek *e-business*.¹⁹

Di Bandung, kasus *cyber crime* berhasil diungkap oleh Kepolisian Daerah (Polda) Jawa Barat. Tujuh pelaku *carding*, pembobolan kartu kredit melalui internet, berhasil diringkus polisi beserta penadahannya. Para pelaku sebagian besar oknum mahasiswa universitas swasta di Bandung. Para pelaku mengaku, perbuatan itu awalnya iseng belaka. Berkembangnya *cyber crime* di kota-kota besar ditunjang oleh ketiadaan perangkat hukum yang mengatur dan sanksi tegas di bidang *cyber*. Pelanggaran di bidang *cyber* dihukum ringan, maksimal setahun, seperti yang terjadi pada pelaku *carding* di Jakarta. Polisi dan jaksa mendakwa pelaku dengan pasal pidana pencurian karena perangkat hukum khusus tentang *cyber crime* belum ada.²⁰

Kejahatan ini sangat menurunkan citra dan nama bangsa Indonesia, karena pemesanan barang melalui internet *e-business* dari berbagai negara dilakukan dengan kartu kredit palsu. Apabila fenomena ini tidak segera diatasi, maka dapat mengurangi kepercayaan dunia terhadap Indonesai. Ujung-ujungnya Indonesia dapat diisolasi dalam kancan perdagangan dunia internasional.

2) Berpotensi menghancurkan negara

Perkembangan teknologi informasi membawa dampak lain, yaitu tumbuh suburnya *cyber crime*, kejahatan melalui internet. *Cyber crime* menjadi masalah serius yang harus ditangani. Kepolisian dan aparat penegak hukum lainnya harus peduli terhadap dampak yang ditimbulkan kejahatan ini dan berupaya serius

¹⁹*Ibid.*

²⁰*Ibid.*, h. 92.

untuk menanggulangnya. Tidak ada negara satu pun di dunia ini yang terbebas—kan dari ancaman *cyber crime*. Hal ini karena kemampuan teknologi internet mengaburkan batas-batas fisik dan budaya sebuah negara.

Pencegahan terhadap tindak pidana *cyber crime*, harus mencakup semua operasi ilegal atau akses ke internet yang merugikan pihak lain. Operasi ilegal itu meliputi akses tanpa izin, merusak data atau program komputer, melakukan sabotase untuk menghilangkan sistem atau jaringan komputer, mengambil data dari dan ke dalam jaringan komputer tanpa izin, serta memata-matai komputer.

3) Keresahan masyarakat pengguna jaringan komputer

Menurut TB Ronny Nitibaskara, kejahatan tidak dapat dilepaskan dari lima faktor, yaitu:

- a) Pelaku Kejahatan,
- b) Modus Kejahatan,
- c) Korban Kejahatan,
- d) Reaksi Sosial atas Kejahatan,
- e) Hukum.

Terkait dengan lima faktor tersebut, Sutanto dan kawan-kawan telah menjelaskan lebih lanjut dengan mengaitkannya pada perkembangan *cyber crime* sebagai kejahatan berdimensi baru. Sutanto dan kawan-kawan menyatakan bahwa pengetahuan tentang *cyber crime* dapat dijelaskan sebagai berikut:²¹

a) Pelaku Kejahatan

Dalam hal pelaku kejahatan maya (*cyber crime*), sudah disinggung bahwa karakter “subyek hukum” berbeda dari pelakunya. Dalam *cyber crime*, pelaku

²¹Sutanto, Hermawan Sulistyio dan Tjuk Sugiarto dalam Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya* (Cet. I; Yogyakarta: Laksbang Pressindo, 2007), h. 95.

terlihat memiliki keunikan-keunikan tersendiri, yang belum tertampung dalam konsep-konsep atau teori konvensional mengenai tindak kejahatan.

b) Modus Kejahatan

Bahwa modus operandi *cyber crime* sangat berbeda dari tindak kejahatan konvensional. Yang paling mencolok dari perbedaan tersebut antara lain adalah *locus delicti* (tempat kejahatan perkara) karena sangat sulit melokalisasi jaringan internet.

c) Korban Kejahatan

Korban *cyber crime* tidak selalu dalam bentuk yang dilihat (*tangible*) melainkan juga yang tidak terlihat (*intangible*). Karena tempat tinggal dan kewarganegaraan korban yang tidak selalu sama dengan pelaku *cyber crime*, maka penegak hukum menghadapi masalah yang jauh lebih kompleks.

d) Reaksi Sosial atas Kejahatan

Pada kejahatan konvensional, reaksi sosial atas suatu tindak kejahatan jauh lebih terukur ketimbang yang terjadi pada kasus *cyber crime*. Misalnya, reaksi massa terhadap perampok atau pencuri yang tertangkap berupa penghakiman massa. Sebaliknya, segmen masyarakat yang bereaksi atas suatu tindak *cyber crime* tidak sebesar pada kasus kejahatan konvensional. Namun demikian, dampak *cyber crime* tidak lebih kecil dibandingkan dengan dampak kejahatan konvensional.

e) Hukum

Undang-undang dan perangkat hukum serta aturan lain yang bersifat empirik hingga saat ini masih banyak di antaranya yang bersandar pada yurisprudensi. Sebaliknya, *cyber crime* perlu waktu dalam proses beradaptasi, karena sistem

hukum *cyber crime* secara universal membutuhkan sinergitas terhadap 3 (tiga) aspek, yakni: aspek struktural, substansial dan kultural. Di samping itu perlu sistem hukum yang kuat di tengah-tengah arus globalisasi terutama perdagangan internasional.

Pelaku *cyber crime* yang pernah tertangkap kebanyakan adalah remaja, bahkan beberapa di antaranya terhitung masih anak-anak. Para pelaku belum menduduki jabatan-jabatan penting di masyarakat. Para pelaku juga jauh dari profil anak jalanan. Pelaku jarang sekali terlibat kenakalan remaja, berawal dari keluarga baik-baik, dan rata-rata cerdas.

Menangani anak-anak semacam ini, jelas memerlukan pendekatan tersendiri. sejauh ini belum ada penelitian yang komprehensif tentang pelaku tindak pidana *cyber crime*. Modus operandi *cyber crime*, dalam penggunaan teknologi informasi. Sifat inilah yang membuat *cyber crime* berbeda dengan tindak pidana lainnya.

Korban *cyber crime* dapat menimpa siapa saja, mulai dari perseorangan, lembaga, kalangan swasta, hingga negara. Karakter lain dari *cyber crime* adalah *non-violence*. Sifat demikianlah yang menyebabkan korban seperti tidak kasat mata, dan *fear of crime* (ketakutan atas kejahatan) tidak mudah timbul. Padahal, kerusakan yang ditimbulkan oleh kejahatan *cyber* dapat lebih dahsyat dari pada kejahatan-kejahatan konvensional.

Reaksi sosial yang semakin keras terhadap *cyber crime* akan mendorong lahirnya pengaturan-pengaturan yang lebih ketat di dunia *cyber space*. Seberapa keras reaksi sosial, sangat bergantung pada seberapa besar *fear of crime* masyarakat dan kepedulian negara terhadap *cyber crime*. *Cyber crime* semakin meningkat, sedangkan penanggulangannya belum memenuhi rasa keadilan, karena terbentur

berbagai persoalan, baik masalah perangkat hukum, peraturannya, dan para penegak hukum yang kurang terampil dalam melakukan tugasnya.

4) Dampak *cyber crime* terhadap keamanan dalam negeri

Ketidaksiapan Indonesia dalam mengantisipasi perkembangan teknologi informasi dalam bentuk struktur dan infrastruktur hukum, bisa berakibat buruk. dan bukan tidak mungkin ancamannya adalah kerawanan sosial dan politik yang ditimbulkan oleh individu-individu yang berperilaku menyimpang. Motif para pelaku bukan *money oriented*, tetapi melemparkan isu-isu yang meresahkan, memanipulasi simbol-simbol kenegaraan, dan partai politik dengan tujuan untuk mengacaukan keadaan agar tidak tercipta suasana yang kondusif.

Selain kerawanan sosial juga bisa muncul pengaruh negatif dari maraknya situs-situs porno yang dapat diakses bebas dan tanpa batas. Pada jangka waktu tertentu, situs-situs itu berpotensi besar merusak moral bangsa. Generasi muda yang tengah haus-hausnya dengan sesuatu yang berbau porno menjadi sasaran empuk bagi para vendor penyedia jasa internet tersebut. Bisa dibayangkan, jika kelak para generasi muda ini mengambil alih ‘estafet’ kepemimpinan maka akan seperti apa dan akan dibawa ke mana arah bangsa ini?

Selain dua bentuk di atas, salah satu yang amat merugikan adalah ulah para *hecker* yang ingin meraih keuntungan secara finansial dari kegiatannya. Mereka berusaha merusak situs-situs perbankan, kartu kredit, toko-toko yang menawarkan barang secara *on line*, lembaga-lembaga keuangan, bursa efek, kurs valuta asing, dengan maksud terjadinya kekacauan dalam bidang perdagangan.

Berkaitan dengan hal-hal tersebut, faktor-faktor lain juga menjadi penyebab meningkatnya tindak pidana *cyber crime* adalah sebagai berikut:

1. Kesadaran Hukum Masyarakat

Proses penegakan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban di dalam kehidupan bermasyarakat. Melalui sistem peradilan pidana dan sistem pemidanaan. Pada dasarnya hak-hak warga negara yang terganggu akibat perbuatan melawan hukum seseorang akan diseimbangkan kembali.

Cyber crime adalah sebuah perbuatan yang tercela dan melanggar kepatutan di dalam masyarakat serta melanggar hukum, meskipun undang-undang secara khusus mengatur *cyber crime*, akan tetapi belum sepenuhnya dapat dipatuhi dan disadari oleh seluruh pengguna layanan teknologi informasi sebagai instrumen hukum. Oleh karena itu, peran masyarakat dalam upaya penegakan hukum terhadap *cyber crime* adalah penting untuk menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan *cyber crime*.

Sampai saat ini, kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *cyber crime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (*lack of information*) masyarakat terhadap jenis kejahatan *cyber crime*. *Lack of information* ini menyebabkan upaya penanggulangan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan (*controlling*) masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cyber crime*.

Mengenai kendala yang pertama yaitu mengenai proses penataan terhadap hukum. Jika masyarakat di Indonesia memiliki pemahaman yang benar akan tindak pidana *cyber crime*, maka baik secara langsung maupun tidak langsung masyarakat akan membentuk suatu pola penataan. Pola penataan ini dapat berdasarkan karena ketakutan akan ancaman pidana yang dikenakan bila melakukan perbuatan *cyber*

crime atau pola penataan ini tumbuh atas kesadaran mereka sendiri sebagai masyarakat hukum.²²

Melalui pemahaman yang komprehensif mengenai *cyber crime*, peran masyarakat menjadi sangat penting dalam upaya pengawasan, ketika masyarakat mengalami *lack of information*, peran mereka akan menjadi mandul. Misalnya, dalam sebuah masyarakat yang *lack of information*, datang seorang mahasiswa yang membawa seperangkat komputer dan di tempatnya yang baru ini, si mahasiswa memesan barang-barang mewah melalui *carding*. Oleh karena masyarakat tidak mengetahui dan memahami *carding*, maka tidak ada kecurigaan atas perbuatan si mahasiswa ini, bahkan sebaliknya masyarakat cenderung terkesan dengan pola tingkah mahasiswa dimaksud.

Lain halnya dengan delik-delik konvensional seperti pencurian. Masyarakat secara umum telah mengetahui apa yang dimaksud dengan pencurian sehingga ketika ada warga masyarakat yang dicurigai akan melakukan pencurian, masyarakat sekitar dapat mengantisipasinya. Atau jika telah terjadi pencurian di dalam suatu

²²Berkaitan dengan pola penataan, dalam sebuah tulisan yang berjudul Tantangan Bagi Pembinaan Hukum Nasional, seorang sarjana hukum menyatakan bahwa: “....pembangunan hukum itu dapat diadakan di sela-sela pembangunan fisik dan mental, dengan terlebih dahulu menentukan tujuan hukum dan perkembangannya, mengadakan suatu analisa deskriptif dan prediktif, dan mengumpulkan data-data tentang hukum yang masih dianggap melekat dalam diri anggota-anggota masyarakat. Menentukan tujuan hukum dan perkembangannya dirasa tidaklah sulit, sebaliknya yang dianggap sulit adalah menetapkan apakah anggota-anggota masyarakat itu dapat menerima atau mengakui tujuan hukum tersebut. Oleh karena taatnya anggota-anggota masyarakat kepada hukum dapat disebabkan oleh dua faktor dominan, yaitu:

Pertama, bahwa tujuan hukum identik dengan tujuan/aspirasi anggota-anggota masyarakat itu atau dengan kata lain taatnya anggota-anggota masyarakat pada hukum adalah karena terdapatnya perasaan keadilan dan kebenaran dalam hukum itu sendiri.

Kedua, karena adanya kekuasaan yang imperatif melekat dalam hukum tersebut, dengan sanksi apabila ada orang yang berani melanggarnya ia akan memperoleh akibat-akibat hukum yang tidak diingini”, sebagaimana dikutip dari Andi Amrullah dalam Soerjono Soekanto, *Pokok-pokok Sosiologi Hukum* (Jakarta: Rajawali Pers, 1980), h. 125-126.

kompleks masyarakat, warga sekitar segera melaporkan kepada aparat kepolisian setempat.

2. Faktor Keamanan

Rasa aman tentunya akan dirasakan oleh pelaku kejahatan (*cyber crime*) pada saat sedang menjalankan “aksinya”. Hal ini tidak lain karena Internet lazim dipergunakan di tempat-tempat yang relatif tertutup, seperti di rumah, kamar, tempat kerja, perpustakaan bahkan di warung internet (warnet). Aktivitas yang dilakukan oleh pelaku di tempat-tempat tersebut sulit untuk diketahui oleh pihak luar. Akibatnya, pada saat pelaku sedang melakukan tindak pidana/kejahatan sangat jarang orang luar mengetahuinya. Hal ini sangat berbeda dengan kejahatan-kejahatan yang sifatnya konvensional, yang mana pelaku akan mudah diketahui secara fisik ketika sedang melakukan “aksinya”.

Demikian pula, ketika pelaku sedang beraksi di tempat terbuka, tidak mudah orang lain mengetahui “aksinya”. Misalnya di warnet yang tidak mempunyai penyekat ruangan, sangat sulit bagi orang awam untuk mengetahui bahwa seseorang sedang melakukan tindak pidana. Orang lain akan beranggapan bahwa pelaku sedang menggunakan komputer untuk keperluan biasa, padahal sebenarnya ia sedang melakukan kejahatan. Kondisi ini akan membuat pelaku menjadi semakin berani. Di samping itu, apabila pelaku telah melakukan tindak pidana, maka dengan mudah pelaku dapat menghapus semua jejak kejahatan yang telah dilakukan mengingat internet menyediakan fasilitas untuk menghapuskan data/file yang ada. Akibatnya pada saat pelaku tertangkap sukar bagi aparat penegak hukum untuk menemukan bukti-bukti kejahatan.

3. Faktor Penegak Hukum

Faktor penegak hukum sering menjadi penyebab maraknya kejahatan siber (*cyber crime*). Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum mengalami kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku, terlebih apabila kejahatan yang dilakukan memiliki sistem pengoperasian yang sangat rumit.

Di samping itu, aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak institusi kepolisian di daerah baik Polrest Maupun Polsek, belum dilengkapi dengan jaringan internet. Perlu diketahui, dengan teknologinya yang sedemikian canggih, memungkinkan kejahatan dilakukan disatu daerah namun akibat yang ditimbulkan dapat terjadi di daerah lain, bahkan hingga ke luar negeri. Jangankan menyelidiki dan menyidik kasus *cyber crime*, mengenal internet pun belum tentu aparat penegak hukum mengetahuinya (khususnya untuk penegak hukum di daerah).²³

²³Dalam laporan hasil penelitian PPITK-PTIK yang berjudul “*Tindak Pidana Teknologi Komunikasi Informasi Cyber Crime dan Upaya Penanggulangannya*”, Jakarta Desember 2003, dinyatakan bahwa dari sejumlah 42 orang responden yang pernah mengikuti pendidikan kursus komputer, hanya ada 1 (satu) orang yang mempunyai kualifikasi sebagai programer dan sisanya sebagai operator saja. Lebih lanjut dinyatakan bahwa secara mayoritas, pengetahuan yang dimiliki oleh penyidik terbatas pada modus operandi *cyber crime* yang berkaitan erat dengan delik konvensional. Sedangkan untuk modus operandi *cyber crime* yang tergolong *new category of crimes* seperti *cyber terrorism* atau *hacking*, hanya ada 2 (dua) orang penyidik dari 110 responden atau sekitar sebesar 0,18% saja yang memenuhi kualifikasi.

Selain penyidik-penyidik yang bekerja di Polda Metro Jaya, para penyidik lain pada umumnya belum mempunyai pengalaman yang cukup dalam hal penanganan kasus *cyber crime* sampai ke tingkat pengadilan dan divonis.

C. Modus Operandi Terjadinya Cyber Crime

Modus kejahatan dalam *cyber crime* sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan teknologi informasi. Sebab, salah satu karakter pokok *cyber crime* adalah penggunaan sarana teknologi informasi dalam modus operandinya. Sifat inilah yang membuat *cyber crime* berbeda dengan tindak pidana lainnya (konvensional).²⁴

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain:

1. Unauthorized Access to Computer System and Service

Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun demikian, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.

Hal ini dapat dilihat dalam kasus Timor Timur. Beberapa *website* milik pemerintah RI dirusak oleh *hacker* pada tanggal 11 Agustus 1999. Kasus yang lain juga pernah terjadi, dimana *hacker* juga telah berhasil menembus masuk ke dalam *data base* berisi data para pengguna jasa *America Online* (AOL), sebuah perusahaan

²⁴Abdul Wahid dan Muhammad Labib, *Kejahatan Mayantara (cyber crime)* (Refika Aditama, Bandung, 2005), h. 41.

Amerika Serikat yang bergerak di bidang *e-commerce* yang memiliki tingkat kerahasiaan tinggi, hal ini dilansir oleh Indonesian Observer pada tanggal, 26 Juni 2000. Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para *hacker*, yang mengakibatkan tidak berfungsinya situs ini beberapa waktu lamanya (<http://www.fbi.org/>).

2. *Illegal Contents*

Merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

3. *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scripless document* melalui Internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

4. *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan

terhadap saingan bisnis yang dokumen ataupun data pentingnya (*data base*) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer).

5. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6. *Offense against Intellectual Property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh, peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7. *Infringements of Privacy*

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.²⁵

²⁵Petrus Reinhard Golose, *Perkembangan Cyber Crime dan Upaya Penanganannya di Indonesia Oleh Polri* . <http://www.4law.co.il/indo1.pdf>. (Diakses pada tanggal, 25 Juni 2010) dalam Hinca IP Panjaitan dkk, *Membangun Cyber Law Indonesia yang demokratis* (Jakarta : IMLPC, 2005).

D. Penanggulangan Cyber Crime Berdasarkan Perundang-undangan di Indonesia

Kejahatan merupakan entitas yang selalu melekat dengan dinamika perkembangan peradaban umat manusia. Kejahatan yang oleh Saparinah Sadli disebut sebagai perilaku menyimpang, selalu ada dan melekat pada setiap bentuk masyarakat; tidak ada masyarakat sepi dari kejahatan.²⁶

Oleh karena itu, upaya penanggulangan kejahatan sesungguhnya merupakan usaha yang terus menerus dan terus berkesinambungan. Semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi, muncul berbagai jenis kejahatan berdimensi baru, yang termasuk didalamnya *cyber crime*. Sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi ketertiban masyarakat.

Akan tetapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab terhadap dampak negatif yang timbul dari kejahatan. Hal ini dikarenakan teknologi yang membawa perubahan dalam masyarakat berkembang begitu pesat, sementara hukum pidana merupakan produk sejarah tertentu berjalan dengan logika sejarah yang menaunginya walaupun dalam batas tertentu mempunyai prediktabilitas atas perkembangan masyarakat.

Menjawab tuntutan dan tantangan komunikasi global melalui ruang maya (*cyber space*), undang-undang yang diharapkan *ius constituendum*, yakni perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap

²⁶Muladi dan Barda Nawawi Arief, *Bunga Rampai Hukum Pidana* (Bandung: Alumni, 1998), h. 148.

permasalahan, termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.

Saat ini, Indonesia telah memiliki undang-undang khusus (*cyber law*) yang mengatur mengenai *cyber crime*, undang-undang yang dimaksud adalah UU ITE. Meskipun demikian demikian undang-undang tersebut belum berjalan secara optimal. Hal ini terjadi karena adanya pasal-pasal yang memiliki multi tafsir. Sehingga dampak dari pasal tersebut menjerat pelaku yang bukan sasaran undang-undang.

Selain undang-undang *cyber crime* tersebut, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cyber crime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

1. Kitab Undang-Undang Hukum Pidana (KUHP)

Dalam upaya menangani kasus-kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cyber crime* antara lain:

- a) Pasal 362 KUHP yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card generator* di internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.

- b) Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.
- c) Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban.
- d) Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan *e-mail* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan *e-mail* ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.
- e) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di internet dengan penyelenggara dari Indonesia.
- f) Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal.

- g) Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di internet, misalnya kasus Sukma Ayu-Bjah, Ariel-Luna Maya atau Ariel-Cut Tari.
- h) Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
- i) Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

2. Undang-Undang Republik Indonesia No. 19 Tahun 2002 tentang Hak Cipta

Menurut Pasal 1 angka (8) Undang-Undang Republik Indonesia No. 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun (Pasal 30).

Harga program komputer/*software* yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual *software* bajakan dengan harga yang sangat murah. Misalnya, program anti virus seharga \$ 50 dapat dibeli dengan harga Rp 20.000,00. Penjualan dengan harga sangat murah dibandingkan dengan *software* asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 perkeping.

Maraknya pembajakan *software* di Indonesia yang terkesan “dimaklumi” tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu “Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah)”.

3. Undang-Undang Republik Indonesia No. 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 angka (1) Undang-Undang Republik Indonesia No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik.

Penyalahgunaan internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan undang-undang ini, terutama bagi para *hacker* yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

- a) Akses ke jaringan telekomunikasi;
- b) Akses ke jasa telekomunikasi;
- c) Akses ke jaringan telekomunikasi khusus.

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada *website* KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi “Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)”

4. Undang-Undang Republik Indonesia No. 8 Tahun 1997 tentang Dokumen Perusahaan

Dengan dikeluarkannya Undang-Undang Republik Indonesia No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya *Compact Disk - Read Only Memory* (CD - ROM), dan *Write - Once - Read - Many* (WORM), yang diatur dalam Pasal 12 undang-undang tersebut sebagai alat bukti yang sah.

5. Undang-Undang Republik Indonesia No. 25 Tahun 2003 tentang Perubahan atas Undang-Undang Republik Indonesia No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-undang ini merupakan undang-undang yang paling tepat bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas

dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan. Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan. Dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat diperoleh dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data-data tersebut. Undang-undang ini juga mengatur mengenai alat bukti elektronik (*digital evidence*) sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

6. Undang-Undang Republik Indonesia No. 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Selain Undang-Undang Republik Indonesia No. 25 Tahun 2003, undang-undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. *Digital*

evidence atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah *e-mail* dan *chat room* selain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin board* atau *mailing list*.

E. Unsur-unsur Tindak Pidana dalam Cyber Crime

Mengikuti asas yang berlaku dalam hukum pidana, maka seseorang tidak dapat dipersalahkan melakukan tindak pidana apabila tindak pidana tersebut belum dirumuskan di dalam undang-undang.²⁷ Sekalipun perkembangan mutakhir dalam hukum pidana menunjukkan bahwa asas hukum tersebut tidak lagi diterapkan secara rigid atau kaku, tetapi asas hukum tersebut sampai sekarang tetap dipertahankan sebagai asas yang sangat fundamental dalam hukum pidana sekalipun dengan berbagai modifikasi dan pengembangan.²⁸

Dengan demikian seseorang hanya dapat dipersalahkan melakukan tindak pidana apabila orang tersebut melakukan perbuatan yang telah dirumuskan dalam ketentuan undang-undang sebagai tindak pidana. Sejauhmana seseorang melakukan

²⁷Tongat dalam P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia* (Bandung: Citra Aditya Bakti, 1997), h. 151. Bandingkan dengan J.E. Sahetapy, *Hukum Pidana* (Yogyakarta: Liberty, 1995), h. 1. Bandingkan juga dengan Moeljatno, *Asas-Asas hukum Pidana* (Jakarta: Bina Aksara, [t.th]), h. 23.

²⁸Lihat, Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (Bandung: Citra Aditya Bakti, 1996), h. 88.

perbuatan yang telah dirumuskan dalam undang-undang sebagai tindak pidana dapat dipersalahkan melakukan tindak pidana?

Jawaban normatif yang lazim diberikan oleh hukum pidana berdasarkan asas legalitas seperti tersebut di atas adalah, bahwa seseorang hanya dapat dipersalahkan sebagai telah melakukan tindak pidana apabila orang tersebut oleh hakim telah dinyatakan terbukti bersalah dengan memenuhi unsur-unsur dari tindak pidana yang bersangkutan, seperti yang dirumuskan di dalam undang-undang.²⁹

Dengan kata lain dapat dikemukakan, bahwa seseorang tidak dapat dipersalahkan melakukan tindak pidana apabila salah satu unsur tindak pidana yang didakwakan kepada orang tersebut tidak dapat dibuktikan. Sebab tidak terpenuhinya salah satu unsur tindak pidana tersebut membawa konsekuensi dakwaan atas tindak pidana tersebut tidak terbukti. Sekalipun demikian, batasan normatif tersebut dalam perkembangannya mengalami pergeseran, dimana sangat dimungkinkan orang tetap dapat dipersalahkan melakukan suatu tindak pidana berdasarkan nilai-nilai yang hidup dalam masyarakat sekalipun perbuatan tersebut tidak secara tegas diatur dalam perangkat normatif atau undang-undang.³⁰

²⁹P.A.F. Lamintang dan Djisman Samosir, *Delik-delik Khusus Kejahatan yang Ditujukan Terhadap Hak Milik dan Lain-lain Hak yang Timbul Dari Hak Milik* (Bandung: Penerbit Tarsito, 1980), h. 7.

³⁰Dimungkinkannya orang tetap dapat dipersalahkan melakukan tindak pidana sekalipun perbuatan yang dilakukannya itu tidak dirumuskan dalam undang-undang sebagai tindak pidana secara tegas tercantum di dalam ketentuan Pasal 1 ayat (3) Rancangan KUHP Baru Tahun 1992 yang direvisi bulan Maret 1993 yang menyatakan, “Ketentuan dalam ayat (1) tidak mengurangi berlakunya hukum yang hidup yang menentukan bahwa menurut adat setempat seseorang patut dipidana walaupun perbuatan itu tidak diatur dalam peraturan perundang-undangan”. Ketentuan dalam Pasal 1 ayat (3) Rancangan KUHP tersebut yang menyatakan, “Keadilan dan kepastian hukum sebagai tujuan hukum mungkin mendesak dalam penerapan pada kejadian-kejadian nyata.” Dengan menyadari hal tersebut, maka dalam mempertimbangkan hukum yang akan diterapkan hakim sejauh mungkin mengutamakan keadilan (yang tercermin dari nilai-nilai yang hidup) di atas kepastian hukum (yang tercermin dari adanya asas legalitas).

Bertolak dari berbagai tuntutan normatif tersebut, pemahaman terhadap unsur-unsur tindak pidana merupakan kebutuhan yang sangat mendasar berkaitan dengan penerapan hukum pidana materiil.

Secara umum unsur-unsur tindak pidana dapat dibedakan ke dalam dua macam yaitu:

1. Unsur Obyektif, yaitu unsur yang terdapat di luar pelaku (*dader*) yang dapat berupa:
 - a. Perbuatan, baik dalam arti berbuat maupun dalam arti tidak berbuat. Contoh unsur obyektif yang berupa “perbuatan” yaitu perbuatan-perbuatan yang dilarang dan diancam oleh undang-undang. Perbuatan-perbuatan tersebut dapat disebut antara lain perbuatan-perbuatan yang dirumuskan di dalam Pasal 242, 263, 362 KUHP. Di dalam ketentuan Pasal 362 KUHP misalnya, unsur obyektif yang berupa “perbuatan” dan sekaligus merupakan perbuatan yang dilarang dan diancam oleh undang-undang adalah perbuatan mengambil.
 - b. Akibat, yang menjadi syarat mutlak dalam tindak pidana materiil. Contoh unsur obyektif yang berupa suatu “akibat” adalah akibat-akibat yang dilarang dan diancam oleh undang-undang dan sekaligus merupakan syarat mutlak dalam tindak pidana antara lain akibat-akibat sebagaimana dimaksudkan dalam ketentuan Pasal 351, 338 KUHP. Dalam ketentuan Pasal 338 KUHP misalnya, unsur obyektif yang berupa “akibat” yang dilarang dan diancam dengan undang-undang adalah akibat yang berupa matinya orang.
 - c. Keadaan atau masalah-masalah tertentu yang dilarang dan diancam dalam undang-undang.

Contoh unsur obyektif yang berupa suatu “keadaan” yang dilarang dan diancam oleh undang-undang adalah keadaan sebagaimana dimaksud dalam ketentuan Pasal 160, 281 KUHP. Dalam ketentuan Pasal 282 KUHP misalnya, unsur obyektif yang berupa “keadaan” adalah ditempat umum.³¹

2. Unsur Subyektif, yaitu unsur yang terdapat dalam diri si pelaku (*dader*) yang berupa:

a. Hal yang dapat dipertanggungjawabkannya seseorang terhadap perbuatan yang telah dilakukan (kemampuan bertanggung jawab).

b. Kesalahan atau *schuld*

Berkaitan dengan masalah kemampuan bertanggung jawab di atas, persoalannya adalah kapan seseorang dapat dikatakan mampu bertanggung jawab? seseorang dapat dikatakan mampu bertanggung jawab apabila dalam diri orang itu memenuhi tiga syarat, yaitu:

1) Keadaan jiwa orang itu adalah sedemikian rupa, sehingga ia dapat mengerti akan nilai perbuatannya dan karena juga mengerti akan nilai dari akibat perbuatannya itu.

2) Keadaan jiwa orang itu sedemikian rupa, sehingga ia dapat menentukan kehendaknya terhadap perbuatan yang ia lakukan.

3) Orang itu harus sadar perbuatan mana yang dilarang dan perbuatan mana yang tidak dilarang oleh undang-undang.³²

³¹P.A.F. Lamintang dan Djisman Samosir, *op. cit.* Lihat juga, Suharto R.M., *Hukum Pidana Materiil Unsur-unsur Obyektif sebagai Dasar Dakwaan* (Jakarta: Sinar Grafika, 1991), h. 1.

³²Satochid Kartanegara, *Hukum Pidana Kumpulan Kuliah*, Buku I (Jakarta: Balai Lektur Mahasiswa, [t.th.]), h. 242.

Sementara itu berkaitan dengan persoalan kemampuan bertanggung jawab ini pembentuk KUHP berpendirian, bahwa setiap orang dianggap mampu bertanggung jawab.

Konsekuensi dari pendirian ini adalah, bahwa masalah kemampuan bertanggung jawab ini tidak perlu dibuktikan adanya di pengadilan kecuali apabila terdapat keragu-raguan terhadap unsur tersebut.

Bertolak dari pendirian pembentuk KUHP di atas, dapat dimengerti di dalam KUHP sendiri tidak ada penjelasan tentang apa yang dimaksud dengan kemampuan bertanggung jawab. KUHP hanya memberikan rumusan secara negatif atas kemampuan bertanggung jawab ini terdapat di dalam ketentuan Pasal 44 KUHP yang menyatakan kapan seseorang tidak dapat dipertanggungjawabkan atas perbuatannya. Pasal KUHP menyatakan, bahwa seseorang tidak dapat dipertanggungjawabkan atas perbuatannya karena sebab:

a. Jiwanya cacat dalam tubuhnya

Keadaan ini menunjuk pada suatu keadaan dimana jiwa seseorang itu tidak tumbuh dengan sempurna. Termasuk dalam kondisi ini adalah idiot, imbisil, bisu tulis sejak lahir, dan lain-lain.³³

b. Jiwanya terganggu karena suatu penyakit

Dalam hal ini jiwa seseorang itu pada mulanya berada dalam keadaan sehat, tetapi kemudian dihindangi oleh suatu penyakit. Termasuk dalam kondisi ini misalnya maniak, histeria, melankolia, gila dan lain-lain.

³³Lihat, R. Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-komentarnya Lengkap Pasal Demi Pasal* (Bogor: Politeia, Bogor, 1998), h. 8.

Unsur subyektif kedua adalah unsur “kesalahan” atau *schuld*. Sebagaimana diketahui, bahwa kesalahan atau *schuld* dalam hukum pidana dibedakan menjadi dua bentuk, yaitu

- a. *Dolus* atau *opzet* atau kesengajaan.
- b. *Culpa* atau ketidaksengajaan.

Di antara dua unsur subyektif tersebut di atas yang sangat penting berkaitan dengan pembicaraan tentang unsur-unsur tindak pidana adalah kesalahan dalam bentuk “kesengajaan” atau *opzet*. Hal ini disebabkan hampir semua tindak pidana mengandung unsur *opzet*.

Sebagaimana dalam azas-azas hukum pidana umum di dunia nyata hukum pidana mengatur banyak hal tentang kepentingan publik di atas kepentingan pribadi. Hukum pidana mengatur sanksi bagi pelaku tindak pidana dengan hukum badan. Sama halnya di dalam dunia siber (mayantara) unsur-unsur yang ada dalam tindak pidana di bidang ini tidak berbeda, karena yang membedakan hanya modus operandi dan di dalam dunia yang berbedayakni dunia siber. Unsur-unsur tindak pidana dibagi atas 2 (dua):

1. Unsur subyektif, artinya unsur subyektif suatu tindak pidana pelaku dengan maksud atau memang sudah dari awal bermaksud melakukan suatu tindakan melawan hukum. Jadi yang menjadi titik tolak dari jenis kejahatan ini adalah dari pelaku tindak pidana.
2. Unsur obyektif, artinya obyek tindak pidana tersebut bukan setatus miliknya, dan dilakukan melawan hak atau tanpa dan hak mengambil alih, menguasai dan menimbulkan hak atas obyek tersebut.

Jadi, jelas ada dua unsur yang saling mengikat antara unsur obyektif satu dengan yang lain berhubungan dalam dunia siber dapat kita konstruksikan kondisi sebagai berikut:

- Unsur subyektif yakni:
 - *wetwede dat* (yang diketahui)
 - *Opzettelijk* (dengan sengaja)
- Unsur obyektif yakni:
 - *ontrekken* (menjauhkan)
 - *Vergegen* (menyembunyikan)
 - *Eaning goed* (suatu benda)

Karena sifat dari internet juga mengutamakan kerahasiaan baik yang menyangkut rahasia dagang atau informasi rahasia lainnya yang berpotensi dapat disebarkan kepada pihak ketiga tanpa izin pemilik informasi, maka prinsip-prinsip umum di dalam KUHP tidak dapat sepenuhnya dipakaikan dalam menjerat pelaku sebagai bentuk pertanggungjawaban secara pidana.

Dasar pemikiran lain adalah urgensi penggunaan hukum pidana dalam penanggulangan *cyber crime*, jika kriminalisasi suatu perbuatan pidana. Menurut Prof. Nigel Weker, ada beberapa hal yang diperhatikan antara lain:

- a. Kerugian suatu tindak pidana harus jelas termasuk korbannya harus jelas.
- b. Penegakan hukum (*law an forcemant*) harus mendapatkan dukungan masyarakat luas dan dilakukan secara efektif.
- c. Kerugian yang timbul karena pemindahan ini harus lebih kecil dai padacakibat tindak pidana.³⁴

³⁴Robintan Sulaiman, *Cyber Crimes (Perspektif E-Commerce Crime)* (Cet. I; Jakarta: Universitas Pelita Harapan, 2002), h. 90-92.

Unsur melawan hukum (Pasal 1365 KUHPerdara) adalah unsur sangat penting dalam kejahatan siber, sudah barang tentu akan menimbulkan kerugian ekonomis pihak lain akibat dari perbuatannya.

F. Pembuktian Cyber Crime dalam Hukum Pidana di Indonesia

Sistem pembuktian di era teknologi informasi sekarang ini menghadapi tantangan besar yang memerlukan penanganan serius, khususnya dalam kaitan dengan upaya pemberantasan kejahatan di dunia maya (*cyber crime*). Hal ini muncul karena bagi sebagian pihak jenis-jenis alat bukti yang selama ini dipakai untuk menjerat pelaku tindak pidana tidak mampu lagi dipergunakan dalam menjerat pelaku-pelaku kejahatan di dunia maya (*cyber crime*).

Pembuktian dalam hukum pidana merupakan sub sistem kebijakan kriminal sebagai *science of response* yang mencakup berbagai disiplin ilmu. Hal ini disebabkan oleh luasnya kausa dan motif berkembangnya jenis kejahatan yang berbasis teknologi informasi dewasa ini. Penggunaan transaksi elektronik yang tidak menggunakan kertas (*paperles transaction*) dalam sistem pembayaran menimbulkan permasalahan khususnya terkait dengan ketentuan pembuktian sebagaimana diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHPA). Sedangkan dalam Pasal 1866 Kitab Undang-Undang Hukum Perdata (KUHPd) disebutkan alat-alat-alat bukti terdiri atas: bukti tulisan, bukti dengan saksi-saksi, persangkaan, pengakuan dan sumpah.³⁵

³⁵Dikdik M. Arief Mansur dan Alisatris Gultom, *Cyber Law; Aspek Hukum Teknologi Informasi* (Cet. I; Bandung: PT Refika Aditama, 2005), h. 96. Bandingkan dengan Robintan Sulaiman, *Cyber Crimes (Perspektif E-Commerce Crime)* (Cet. I; Jakarta: Pusat Studi Hukum Bisnis Fakultas Hukum Universitas Pelita Harapan, 2002), h. 58.

Pembuktian menurut Pitlot adalah suatu cara yang dilakukan suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya. Menurut Subekti, yang dimaksud dengan pembuktian ialah meyakinkan hakim tentang kebenaran dalil atau dalil-dalil yang dikemukakan dalam suatu persengketaan.³⁶

Menurut Subekti, pembuktian adalah upaya meyakinkan hakim akan hubungan hukum yang sebenarnya antara para pihak dalam perkara, dalam hal ini antara bukti-bukti dengan tindak pidana yang didakwakan. Dalam mengkonstruksikan hubungan hukum ini, masing-masing pihak menggunakan alat bukti untuk membuktikan dalil-dalilnya dan meyakinkan hakim akan kebenaran yang dikemukakan. Untuk itu, hakim patut menerima dalil-dalil para pihak (jaksa ataupun terdakwa) tanpa harus dikungkung oleh batasan alat-alat bukti sepanjang dalil tersebut memenuhi prinsip-prinsip logika.³⁷

Belum hilang dalam ingatan, bahwa aparat penegak hukum dihadapkan pada kesulitan untuk menentukan kualifikasi kejahatan apakah yang dapat dituduhkan pada pelaku *cyber crime*, mengingat sukarnya menemukan alat bukti, seperti yang terlihat dalam kasus mustikaratu.com. Kasus persengketaan antara Tjandra Sugiono dan PT. Mustika Ratu diawali dengan pendaftaran nama domain Mustika Ratu ke Network Solution Inc, di Amerika Serikat. Pada saat itu Tjandra Sugiono menjabat Manajer Umum Pemasaran Internasional PT. Martina Bertho, produsen jamu dan kosmetika Sari Ayu, yang tidak lain adalah pesaing PT. Mustika Ratu dalam industri jamu dan kosmetika. Oleh karena itu, dalam dakwaannya, jaksa penuntut umum menuntut terdakwa telah melakukan suatu bentuk persaingan curang.

³⁶Subekti, *Hukum Pembuktian* (Jakarta: Pradnya Paramita, 1983), h. 7.

³⁷*Ibid.*

Contoh lain berkaitan dengan munculnya persoalan hukum akibat penggunaan produk teknologi informasi dalam proses pemeriksaan perkara pidana adalah penggunaan *teleconference* dalam kasus bom Bali dan kasus korupsi di BULOG (*Bulloggate*). Oleh beberapa pengamat, penggunaan *teleconference* dipandang sebagai suatu terobosan hukum mengingat penggunaan teknologi ini belum diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Sementara itu, pesatnya teknologi informasi melalui internet telah mengubah aktivitas-aktivitas kehidupan yang semula perlu dilakukan secara kontak fisik, kini dengan menggunakan media *cyber space*, aktivitas keseharian dapat dilakukan secara *virtual* atau maya. Masalah pelik yang dihadapi penegak hukum saat ini adalah, bagaimana menjaring pelaku *cyber crime* yang mengusik rasa keadilan tersebut dikaitkan dengan ketentuan pidana yang berlaku?

Hambatan yang klasik adalah sulitnya menghukum pelaku mengingat belum lengkapnya ketentuan pidana yang mengatur tentang kejahatan komputer, internet, dan teknologi informasi (*cyber crime*) dan belum diterimanya dokumen elektronik (misalnya file komputer) sebagai alat bukti oleh konsep yang dianut KUHAP.³⁸

Berhadapan dengan kasus *cyber crime*, pembuktian menjadi masalah yang pelik. Seringkali penegak hukum di Indonesia mengalami kesulitan saat menjerat pelaku *cyber crime* karena masalah pembuktian (*documentary evidence*) yang tidak memenuhi ketentuan sistem hukum pidana Indonesia. Sementara upaya penjeratan

³⁸Mengenai keabsahan transaksi dan kekuatan pembuktian, Mas Wigrantoro Roes Setiyadi dan Minna Dian Avanti Siregar menyatakan bahwa transaksi elektronik tidak memerlukan hard copy atau warkat kertas, namun demikian setiap transaksi yang melibatkan eksekusi diberikan tanda bukti berupa Homer atau kode yang dapat disimpan/direkam di komputer atau dicetak. Permasalahannya muncul ketika terjadi sengketa, apakah bukti/kode nomor transaksi dapat digunakan sebagai alat bukti yang sah menurut hukum Indonesia, mengingat Indonesia belum memiliki ketentuan khusus yang mengatur kegiatan dan transaksi elektronik melalui Internet.

terhadap pelaku-pelaku *cyber crime* harus tetap dilakukan, upaya perluasan bukti menjadi solusi untuk menegakkan hukum.

Dalam sistem hukum pembuktian di Indonesia, terdapat beberapa doktrin pengelompokkan alat bukti, yang membagi alat-alat bukti ke dalam kategori *oral evidence*, *documentary evidence*, *material evidence* dan *electronic evidence*.³⁹ Berikut pembagian pada masing-masing kategori:

1. *Oral Evidence*

- a. Perdata (keterangan saksi, pengakuan, dan sumpah).
- b. Pidana (keterangan saksi, keterangan ahli, dan keterangan terdakwa).

2. *Documentary Evidence*

- a. Perdata (surat dan persangkaan).
- b. Pidana (surat dan petunjuk).

3. *Material Evidence*

- a. Perdata (tidak dikenal).
- b. Pidana (barang yang digunakan untuk melakukan tindak pidana, barang yang digunakan untuk membantu tindak pidana, barang yang merupakan hasil dari suatu

³⁹Freddy Haris, *Cyber Crime* dari Perspektif Akademis, Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia, hlm. 15-16., dalam <http://www.gipi.or.id> akses tanggal 30 Mei 2004. Perlu juga diketahui penyusunan alat-alat bukti di negara-negara *common law*, seperti Amerika Serikat yang berbeda dengan pembagian alat bukti di dalam sistem pembuktian Indonesia. Alat-alat bukti menurut *Criminal Procedure Law* Amerika Serikat yang disebut *forms of evidence* terdiri dari :

- a. *real evidence* (bukti sungguhan);
- b. *documentary evidence* (bukti dokumenter);
- c. *testimonial evidence* (bukti kesaksian);
- d. *judicial notice* (pengamatan hakim).

Tidak disebut alat bukti kesaksian ahli dan keterangan terdakwa. Kesaksian ahli digabungkan dengan bukti kesaksian. Yang lain daripada yang tercantum dalam KUHAP Indonesia ialah *real evidence* yang berupa objek materiel. *Real evidence* ini biasa disebut bukti yang berbicara untuk diri sendiri. Bukti bentuk ini dipandang paling bernilai dibanding bukti yang lain. sebagaimana dikutip dari Andi Hamzah, *Hukum Acara Pidana Indonesia* (Edisi Revisi, Jakarta, Sinar Grafika, 2000), h. 254-255.

tindak pidana, barang yang diperoleh dari suatu tindak pidana, dan informasi dalam arti khusus).

4. *Electronic Evidence*

- a. Konsep pengelompokkan alat bukti menjadi alat bukti tertulis & elektronik. Tidak dikenal di Indonesia
- b. Konsep tersebut terutama berkembang di negara-negara *common law*.
- c. Pengaturannya tidak melahirkan alat bukti baru, tetapi memperluas cakupan alat bukti yang masuk kategori *documentary evidence*.

Di dalam Hukum Acara Pidana, dikenal 5 (lima) alat bukti yang sah sebagaimana diatur dalam pasal 184 ayat 1 KUHAP. Di luar alat-alat bukti ini, tidak dibenarkan dipergunakan sebagai alat bukti untuk membuktikan kesalahan terdakwa. Hakim ketua sidang, penuntut umum, terdakwa, atau penasehat umum terikat dan terbatas hanya diperbolehkan mempergunakan alat-alat bukti ini saja. Mereka tidak leluasa mempergunakan alat bukti yang dikehendakinya diluar alat bukti yang ditentukan pada pasal 184 ayat 1 KUHAP.⁴⁰ Alat-alat bukti yang dimaksud adalah:

1. Keterangan saksi-saksi

Dalam Pasal 185 KUHAP ayat 1 disebutkan bahwa keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan di sidang pengadilan. Dalam penjelasan KUHAP dinyatakan bahwa dalam keterangan saksi tidak termasuk keterangan yang diperoleh dari orang lain (*testimonium de auditu*).

⁴⁰M. Yahya Harahap, *op. cit.*, h. 807. Selanjutnya dinyatakan dalam M. Yahya Harahap bahwa yang dinilai sebagai alat bukti dan yang dibenarkan mempunyai kekuatan pembuktian hanya terbatas pada alat-alat bukti yang disebut pasal 184 ayat 1 KUHAP. Pembuktian dengan alat bukti di luar jenis alat bukti tersebut, sama sekali tidak mempunyai nilai serta tidak mempunyai kekuatan pembuktian yang mengikat.

Pasal 1 angka 27 KUHAP menyatakan bahwa keterangan saksi adalah salah satu alat bukti dalam perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar sendiri, ia lihat sendiri dan ia alami sendiri dengan menyebut alasan dari pengetahuannya itu. Menurut Andi Hamzah, sesuai dengan penjelasan Pasal 185 ayat 1 KUHAP tersebut dan selaras pula dengan tujuan hukum acara pidana yaitu mencari kebenaran materiil, dan pula untuk perlindungan terhadap hak-hak asasi manusia, di mana keterangan seorang saksi yang hanya mendengar dari orang lain, tidak terjamin kebenarannya, maka kesaksian *de auditu* atau *hearsay evidence* patut tidak dipakai di Indonesia.⁴¹

Sementara itu argumentasi dari golongan yang pro dan kontra mengenai kesaksian *de auditu* sebagai alat bukti yang membawa pada kesimpulan bahwa perlu diberikan jawaban yang jelas apa yang dimaksud dengan kesaksian *de auditu* atau *hearsay evidence* itu. Di mana pun pengakuan terhadap *hearsay* sebagai alat bukti tergantung pada tujuan untuk apa hal itu diajukan dan apa yang akan dibuktikan dengan itu. Pada umumnya *hearsay* diterima sebagai alat bukti tetapi dibatasi pengertiannya dari pengertian biasa. Tidak diajukan sebagai *hearsay*, misalnya keterangan terdakwa bahwa seseorang telah mengakui kepadanya bahwa orang itulah yang melakukan kejahatan tersebut.⁴²

2. Keterangan Ahli

Pasal 186 KUHAP menyatakan bahwa keterangan seorang ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Selanjutnya penjelasan pasal 186 KUHAP menyatakan bahwa keterangan ahli ini dapat juga sudah diberikan pada

⁴¹Andi Hamzah, *op. cit.*, h. 260.

⁴²*Ibid.*, h. 264-265.

waktu pemeriksaan oleh penyidik atau penuntut umum yang dituangkan dalam suatu bentuk laporan dan dibuat dengan mengingat sumpah di waktu ia menerima jabatan atau pekerjaan.

KUHAP membedakan keterangan seorang ahli di persidangan sebagai alat bukti "keterangan ahli" dan keterangan seorang ahli secara tertulis di luar sidang pengadilan sebagai alat bukti "surat" (Pasal 187 butir c KUHAP), contoh yang kedua ialah *visum et repertum* yang dibuat oleh seorang dokter.⁴³

Menurut teori hukum pidana yang dimaksud dengan keterangan ahli adalah keterangan yang diberikan seseorang berdasarkan ilmu dan pengetahuan yang dikuasainya.

3. Surat

Alat bukti surat diatur dalam Pasal 187 KUHAP. Dalam komentar KUHAP yang disusun oleh M. Karjadi dan R. Soesilo sebagaimana di tulis oleh Dikdik M. Arief Mansur dan Elisatris Gultom, Pasal 187 membedakan atas empat macam surat, yaitu:

- a. Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat di hadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau dialaminya sendiri, disertai dengan alasan tentang keterangan itu;
- b. Surat yang dibuat menurut peraturan undang-undang atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukkan bagi pembuktian sesuatu hal atau keadaan;

⁴³ *Ibid.* h. 269.

- c. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai suatu hal atau keadaan yang diminta secara resmi dari padanya; dan
- d. Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.⁴⁴

4. Petunjuk

Pasal 188 ayat 1 KUHAP memberi definisi petunjuk sebagai perbuatan, kejadian atau keadaan, yang karena penyesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya. Selanjutnya dalam pasal 188 ayat 3 KUHAP dinyatakan bahwa penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan arif lagi bijaksana, setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan keseksamaan berdasarkan hati nuraninya.

Berdasarkan Pasal 188 ayat 3 KUHAP tersebut, Andi Hamzah menjelaskan bahwa pada akhirnya persoalannya diserahkan kepada hakim. Dengan demikian menjadi sama dengan pengamatan hakim sebagai alat bukti. Apa yang disebut pengamatan oleh hakim (*eigen warmeming van de rechter*) harus dilakukan selama sidang, apa yang telah dialami atau diketahui oleh hakim sebelumnya tidak dapat dijadikan dasar pembuktian, kecuali kalau perbuatan atau peristiwa itu telah diketahui oleh umum.⁴⁵

⁴⁴M. Karjadi dan R. Soesilo, *Kitab Undang-Undang Hukum Acara Pidana dengan Penjelasan Resmi dan Komentar serta Peraturan Pemerintah R.I. No. 27 Tahun 1983 tentang Pelaksanaannya* (Bogor: Politeia, 1997), h. 166.

⁴⁵Andi Hamzah, *op. cit.*, h. 272.

5. Keterangan Terdakwa

Keterangan terdakwa menurut Pasal 189 ayat 1 adalah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. Keterangan terdakwa tidak perlu sama dengan pengakuan, karena pengakuan sebagai alat bukti mempunyai syarat; (a) mengaku ia yang melakukan delik yang didakwakan dan (b) mengaku ia bersalah. Keterangan terdakwa sebagai alat bukti lebih luas pengertiannya dari pengakuan terdakwa.⁴⁶

Berkaitan dengan alat-alat bukti tersebut, maka sepatutnya tidak mengabaikan asas umum sebagai landasan pokok dalam hukum pembuktian sebagaimana hal ini juga berlaku dalam *cyber crime*, karena *cyber crime* adalah bersifat khusus (*lex specialis*). Akan tetapi atasnya tetap diharuskan untuk mengacu kepada asas-asas pembuktian yang umum juga. Beberapa asas dalam hukum acara perdata mengenai pembuktian, yaitu:

1. Asas *Audi et alteram partem*, yaitu bahwa kedua belah pihak yang bersengketa harus diperlakukan sama atau dalam praktik dikenal dengan “*equal justice before the law*”.
2. Gugatan harus diajukan pada pengadilan dimana tergugat bertempat tinggal atau dikenal dengan “*Actor sequitor forum rei*”.

⁴⁶*Ibid.*, h. 273. Lebih lanjut mengenai keterangan terdakwa, dinyatakan dalam Andi Hamzah bahwa menurut Memorie van Toelichting Ned. Sv, penyangkalan terdakwa boleh juga menjadi alat bukti yang sah. Mengenai hal ini D. Simon mengajukan keberatannya, karena hak kebebasan terdakwa untuk mengaku atau menyangkal harus dihormati. Oleh sebab itu, D. Simon berpendapat bahwa suatu penyangkalan terhadap suatu perbuatan mengenai suatu keadaan tidak dapat dijadikan bukti. Sementara itu Andi Hamzah menyatakan bahwa suatu hal yang jelas berbeda antara “keterangan terdakwa” sebagai alat bukti dengan “pengakuan terdakwa” ialah bahwa keterangan terdakwa yang menyangkal dakwaan, tetapi membenarkan beberapa keadaan atau perbuatan yang menjurus kepada terbuktinya perbuatan sesuai alat bukti lain merupakan alat bukti.

Asas tersebut dikembangkan bertolak dari apa yang dikenal dalam hukum pidana dengan “*Presumption of innocence*”.

3. Asas *Actori incumbit probatio*, yaitu bahwa siapa yang mengaku memiliki hak harus membuktikannya. Asas ini berdasarkan kepada apa yang tampak telah ada secara sah haruslah untuk sementara dibiarkan dalam keadaan demikian untuk kepastian hukum. Namun demikian yang harus dibuktikan tersebut hanyalah yang positif saja, yaitu adanya suatu peristiwa dan bukan tidak adanya peristiwa.⁴⁷

Dalam sistem pembuktian terdapat macam-macam sistem atau teori pembuktian. Sistem atau teori pembuktian tersebut adalah:

1. Sistem atau teori pembuktian berdasar undang-undang secara positif

Pembuktian yang didasarkan kepada alat-alat pembuktian yang disebut undang-undang disebut sistem atau teori pembuktian berdasarkan undang-undang secara positif (*positief wettelijk bewijstheorie*). Artinya jika tidak terbukti suatu perbuatan sesuai alat-alat bukti yang disebut undang-undang, maka keyakinan hakim diabaikan.

2. Sistem atau teori pembuktian berdasar undang-undang secara negatif

Teori ini menyandarkan bahwa hakim dalam mengambil keputusan tentang salah atau tidaknya seorang terdakwa terikat oleh alat bukti yang ditentukan oleh undang-undang dan keyakinan hakim sendiri. Dalam sistem ini ada dua hal yang merupakan syarat untuk membuktikan kesalahan terdakwa, yakni adanya alat bukti yang sah yang telah diterapkan dan adanya keyakinan hakim berdasarkan bukti-bukti tersebut hakim meyakini kesalahan terdakwa. Berdasarkan pasal 183 KUHP,

⁴⁷Isis Ikhwanasyah, *Prinsip-prinsip Universal Bagi Kontrak Melalui E-Commerce dan Sistem Hukum Pembuktian Perdata dalam Teknologi Informasi*, dalam *Cyber Law: Suatu Pengantar* (ELIPS, Bandung, 2002), h. 36.

sistem pembuktian yang dianut dalam KUHAP adalah sistem atau teori pembuktian berdasar undang-undang secara negatif.⁴⁸

4. Sistem atau teori pembuktian berdasar keyakinan hakim (*conviction in time*)

Berdasar teori ini, di dalam menjatuhkan putusannya Hakim tidak terikat dengan alat bukti yang ada. Darimana hakim menyimpulkan putusannya tidaklah menjadi masalah, karena ia dapat menyimpulkan dari alat bukti yang ada dalam persidangan atau mengabaikan alat bukti yang ada dalam persidangan.

4. Sistem atau teori pembuktian berdasarkan keyakinan hakim atas alasan yang logis (*conviction raisonnee*)

Menurut teori ini, hakim dapat memutuskan seseorang bersalah berdasarkan keyakinannya, keyakinan mana didasarkan kepada dasar-dasar pembuktian disertai dengan suatu alasan-alasan yang logis. Sistem atau teori pembuktian ini disebut juga pembuktian bebas karena hakim bebas untuk menyebut alasan-alasan keyakinannya. Indonesia sendiri menganut sistem ini dalam pembuktiannya.

Dalam pengungkapan suatu perkara pidana, paling tidak ada tiga hal yang tidak dapat dipisahkan karena menyangkut keabsahan atau kevalidan suatu putusan pengadilan, yaitu: sistem pembuktian yang dianut oleh hukum acara, alat bukti dan kekuatan pembuktian serta barang bukti yang akan memperkuat alat bukti yang dihadirkan di dalam sidang pengadilan. Sehingga membuktikan berarti memberi

⁴⁸Pasal 183 KUHAP selengkapnya berbunyi: “Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya.” Atas pasal ini dapat dilihat bahwa putusan hakim haruslah didasarkan kepada minimum dua alat bukti dan dari alat bukti tersebut hakim harus memperoleh keyakinan bahwa terdakwa bersalah melakukan tindak pidana. Meskipun di dalam persidangan telah diajukan dua atau lebih barang bukti namun bila hakim tidak yakin bahwa terdakwa bersalah, maka terdakwa tersebut harus dibebaskan.

kepastian kepada hakim tentang adanya peristiwa-peristiwa tertentu. Baik dalam hukum acara perdata maupun dalam hukum acara pidana, pembuktian memegang peranan yang sangat sentral.⁴⁹

Hukum pidana menganggap bahwa pembuktian merupakan bagian yang sangat esensial untuk menentukan nasib seseorang terdakwa.⁵⁰ Bersalah atau tidaknya seorang terdakwa sebagaimana yang didakwakan dalam surat dakwaan ditentukan pada proses pembuktiannya. Dengan kata lain pembuktian merupakan suatu upaya untuk membuktikan kebenaran dari isi surat dakwaan yang disampaikan oleh para jaksa penuntut umum, yang kegunaannya untuk memperoleh kebenaran sejati/materiil terhadap:

1. Perbuatan-perbuatan manakah yang dianggap terbukti menurut pemeriksaan persidangan.
2. Apakah telah terbukti bahwa terdakwa bersalah atas perbuatan-perbuatan yang didakwakan kepadanya.
3. Tindak pidana apakah yang dilakukan sehubungan dengan perbuatan-perbuatan itu.
4. Hukuman apakah yang harus dijatuhkan kepada terdakwa bukan pekerjaan mudah.⁵¹

Berkenaan dengan hukum pembuktian dalam proses peradilan baik dalam perkara pidana maupun perdata, kemajuan teknologi khususnya teknologi informasi, memunculkan persoalan tersendiri mengenai apakah hukum pembuktian yang ada

⁴⁹Edmund Makarim, *Kompilasi Hukum Telematika* (Jakarta: Divisi Buku Perguruan Tinggi, PT RajaGrafindo Persada, 2003), h. 419.

⁵⁰*Ibid.*

⁵¹*Ibid.*, h. 420.

saat ini telah mampu menjangkau pembuktian kasus-kasus *cyber crime*. Kedudukan produk teknologi, khususnya catatan/dokumen elektronik masih menjadi bahan perdebatan mengenai bagaimana kedudukannya sebagai alat bukti yang sah di persidangan.

Dalam kaitannya dengan hubungan hukum yang terjadi di *cyber space*, yang menjadi pertanyaan adalah apakah untuk pembuktian tentang berbagai peristiwa hukum yang terjadi di *cyber space* dapat diterapkan kaidah-kaidah hukum di dunia non virtual?

Lahirnya Undang-Undang ITE menjadi babak baru dalam sistem perundang-undangan dan sistem hukum di Indonesia. Hal ini karena alat bukti dalam dunia *cyber* telah memperluas pembuktian dalam tindak pidana di dunia maya (*cyber crime*).

Dalam sistem hukum pidana di Indonesia pengaturan alat bukti telah diatur di dalam undang-undang yang berlaku. Berkaitan dengan pembuktian *cyber crime*, diatur dalam Undang-Undang ITE Pasal 44. Pasal tersebut menyatakan, alat bukti penyidikan, penuntutan dan pemeriksaan disidang pengadilan menurut ketentuan undang-undang ini adalah alat bukti sebagaimana diatur dalam ketentuan perundang-undangan dan alat bukti berupa informasi elektronik dan/atau dokumen elektronik.

Informasi elektronik adalah salah satu atau sekumpulan data elektronik, yang tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange (EDI)*, surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Sedangkan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirim, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, yang tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang memiliki makna (arti) atau dapat dipahami oleh orang yang mampu memahaminya.

Selanjutnya pada Pasal 5 Ayat (1), (2), (3), dan (4) dalam Undang-Undang ITE menyatakan bahwa: informasi elektronik dan/atau data elektronik hasil cetaknya dapat dijadikan sebagai alat bukti hukum yang sah sekaligus merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.

Uraian sebagaimana tersebut di atas merupakan akses dalam melakukan pembuktian dalam kejahatan *cyber crime* sekaligus upaya *law an forcement* dalam mengatasi kejahatan berbasis dunia *cyber*. Sampai saat ini pembuktian yang masih menggunakan ketentuan hukum yang lama tetapi masih relevan dengan pembuktian saat ini masih dapat pula digunakan sebagai bagian dari alat bukti yang sah. Hal ini dapat dilihat dalam Undang-Undang Republik Indonesia No. 8 Tahun 1997 tentang Dokumen Perusahaan.⁵² Namun demikian keberadaan Undang-Undang Dokumen Perusahaan dapat menjangkau ke arah pembuktian data elektronik.⁵³

Meskipun Undang-Undang Dokumen Perusahaan tidak mengatur masalah pembuktian, namun melalui undang-undang ini, pemerintah berusaha mengatur

⁵²Undang-Undang Republik Indonesia No. 8 Tahun 1997 tentang Dokumen Perusahaan selanjutnya disebut Undang-Undang Dokumen Perusahaan.

⁵³Isis Ikhwansyah, *op. cit*, h. 33.

pengakuan atas *microfilm* dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan, misalnya *Compact Disk-Read Only Memory* (CD-ROM) dan *Write-One-Read-Many* (WORM), yang diatur dalam Pasal 12 Undang-Undang Dokumen Perusahaan sebagai alat bukti yang sah.⁵⁴

Pasal 12 dalam Undang-Undang Dokumen Perusahaan tersebut menyatakan sebagai berikut:

1. Dokumen perusahaan dapat dialihkan ke dalam *microfilm* atau media lainnya.
2. Pengalihan dokumen perusahaan ke dalam *microfilm* atau media lainnya sebagaimana dimaksud dalam ayat 1 dapat dilakukan sejak dokumen tersebut dibuat atau diterima oleh perusahaan yang bersangkutan.
3. Dalam mengalihkan dokumen perusahaan sebagaimana dimaksud dalam ayat 1, pimpinan perusahaan wajib mempertimbangkan kegunaan naskah asli dokumen yang perlu tetap disimpan karena mengandung nilai tertentu demi kepentingan perusahaan atau demi kepentingan nasional.
4. Dalam hal dokumen perusahaan yang dialihkan ke dalam *microfilm* atau sarana lainnya adalah naskah asli yang mempunyai kekuatan hukum pembuktian otentik dan masih mengandung kepentingan hukum tertentu, pimpinan perusahaan wajib tetap menyimpan naskah asli tersebut.

Di samping itu, Pasal 3 Undang-Undang Tentang Dokumen Perusahaan telah memberi peluang luas terhadap pemahaman atas alat bukti, yaitu: “Dokumen

⁵⁴Di dalam RUU *Cyber Law* Indonesia, istilah “dokumen elektronik” merujuk kepada “*electronic records*”. Jadi dokumen elektronik di sini tidak sekedar berkas atau *file* saja. Dokumen elektronik yang sah harus ditandatangani (secara digital). sebagaimana dikutip dari Budi Rahardjo, Tema, *Pemik Peraturan dan Pengaturan Cyber Space di Indonesia*, Draft Buku *Cyber Law* Versi 2.3, 2003, diakses dari <http://www.budi.insan.co.id> pada tanggal 21 Maret 2005.

Keuangan terdiri dari catatan, bukti pembukuan, dan data pendukung administrasi keuangan, yang merupakan bukti adanya hak dan kewajiban serta kegiatan usaha suatu perusahaan.”

Selanjutnya, Pasal 4 Undang-Undang Tentang Dokumen Perusahaan menyatakan “dokumen lainnya terdiri dari data atau setiap tulisan yang berisi keterangan yang mempunyai nilai guna bagi perusahaan meskipun tidak terkait langsung dengan dokumen perusahaan.”

Sebuah dokumen perusahaan baru mempunyai kekuatan sebagai alat bukti setelah dilakukan proses pengalihan yang kemudian dilanjutkan dengan proses legalisasi, yang diatur dalam Pasal 13 dan 14 Undang-Undang Dokumen Perusahaan. Setelah proses pengalihan dan legalisasi, dokumen perusahaan tersebut dinyatakan sebagai alat bukti yang sah, sebagaimana disebutkan dalam Pasal 15 Undang-Undang Dokumen Perusahaan.

Berkenaan dengan hukum pembuktian dalam proses peradilan baik dalam perkara pidana maupun perdata, akibat kemajuan teknologi khususnya teknologi informasi, ada suatu persoalan mengenai bagaimana kedudukan produk teknologi, khususnya catatan elektronik, sebagai alat bukti. Sebagai contoh, penggunaan *teleconference* dalam persidangan oleh beberapa kalangan dipandang sebagai terobosan hukum atau penemuan hukum karena penggunaan teknologi ini belum diatur dalam KUHAP. Di mana KUHAP telah jelas menentukan keharusan kehadiran saksi dalam persidangan. Keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan di sidang pengadilan. Dalam hal penggunaan *televideoconference*, kehadiran saksi di sidang pengadilan bukan secara fisik, namun secara virtual. Hal

inilah yang masih menimbulkan pro dan kontra apakah kehadiran secara *virtual* ini dapat disetarakan dengan kehadiran fisik.⁵⁵

Mengenai keabsahan transaksi dan kekuatan pembuktian, transaksi elektronik tidak memerlukan *hard copy* atau warkat kertas, namun demikian setiap transaksi yang melibatkan eksekusi diberikan tanda bukti berupa nomor atau kode yang dapat disimpan/direkam di komputer atau dicetak. Permasalahannya muncul ketika terjadi sengketa, apakah bukti/kode nomor transaksi dapat digunakan sebagai alat bukti yang sah menurut hukum Indonesia, mengingat Indonesia belum memiliki ketentuan khusus yang mengatur kegiatan dan transaksi elektronik melalui internet.⁵⁶

Sementara belum ada peraturan perundang-undangan yang khusus mengatur masalah ini, Sundari berpendapat bahwa, sesuai Pasal 1338 Kitab Undang-Undang Hukum Perdata, perjanjian di antara bank dan nasabah mengikat kedua belah pihak dan berlaku seperti undang-undang bagi kedua belah pihak (*pacta sun servanda*), sehingga bukti/kode nomor transaksi yang dipegang oleh kedua belah pihak tersebut dapat diperlakukan sebagai alat bukti yang sah.⁵⁷

⁵⁵Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, *loc. cit.*, h. 35.

⁵⁶*Ibid.* Lebih lanjut Menurut Edmon Makarim dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) juga mengatur *e-documents* untuk bisnis seperti *invoice*, *quotation*, *bill of lading*, *payment instruction*, bukti pembayaran, *delivery order*, *purchase order* dan lain-lain dalam bentuk elektronik. secara khusus, Undang-Undang ITE juga mengatur secara rinci mengenai tanda tangan elektronik. Undang-Undang ITE menjadi landasan bagi peraturan perundang-undangan lainnya, seperti bea materai elektronik, *e-Government*, revisi undang undang pasar modal, peraturan perpajakan *online*, peraturan tegas mengenai *online banking*, dan peraturan sektoral. Ini penting untuk menghapus keraguan terhadap peraturan perundang-undangan lama yang belum memberikan pengakuan terhadap informasi elektronik, transaksi elektronik dan tanda tangan elektronik. Sebagaimana dikutip dari “*Mengatur Dunia Rimba Raya* (eBizz Asia, Volume 1 Nomor 09, Juli 2003.

⁵⁷Mas Wigrantoro Roes Setiyadi dan Minna Dian Avanti Siregar, *loc. cit.*, h. 36.

Pengakuan catatan transaksi elektronik sebagai alat bukti yang sah di pengadilan sudah dirintis oleh *United Nation Commission on International Trade* (UNCITRAL) yang mencantumkan dalam *e-commerce model law* ketentuan mengenai transaksi elektronik diakui sederajat dengan “tulisan” di atas kertas sehingga tidak dapat ditolak sebagai bukti pengadilan. Mengacu pada ketentuan UNCITRAL, ada peluang bagi Indonesia untuk menempatkan tanda tangan atau bukti elektronik sebagai alat bukti yang sah, sepanjang ditetapkan dalam undang-undang yang khusus mengatur soal transaksi elektronik. Pasal 5 dan 6 dalam Undang-Undang ITE menyatakan bahwa transaksi yang dilakukan dengan memanfaatkan media elektronik memiliki nilai yang sama dengan tulisan atau akta yang dibuat secara konvensional, sehingga pada praktiknya tidak dapat ditolak suatu bukti transaksi yang dilakukan secara elektronik.

Sementara itu, hukum pembuktian di Belanda (sebagai sesama negara yang menganut Sistem Eropa Kontinental)⁵⁸ telah mulai meninggalkan penyebutan alat-alat bukti secara limitatif. Pasal 197 BRV (*Burgerlijke Reglement op de Rechtsvordering*) sebagai pasal penting dalam hukum pembuktian Belanda, menyatakan bahwa pembuktian dapat dilakukan dengan cara apapun, kecuali undang-undang menentukan lain. Selanjutnya, penilaian terhadap bukti yang

⁵⁸Sistem hukum ini berkembang di Eropa Daratan yang juga disebut sebagai “civil law”. Hukum ini awalnya berasal dari kodifikasi hukum yang berlaku di kekaisaran Romawi pada masa pemerintahan Justinianus abad VI Sebelum Masehi. Peraturan-peraturan hukumnya merupakan kumpulan pelbagai kaidah hukum yang ada sebelum Justinianus yang kemudian disebut “*corpus juris civilis*”. Jadi, sistem Hukum Eropa Kontinental adalah suatu sistem hukum dengan ciri-ciri adanya berbagai ketentuan-ketentuan hukum dikodifikasi (dihimpun) secara sistematis yang akan ditafsirkan lebih lanjut oleh hakim dalam penerapannya. Filosofi sistem Hukum Eropa Kontinental tampak pada sifat-sifatnya yang represif, yang senantiasa cenderung melindungi yang berkuasa. Hal ini bisa dimaklumi karena yang berkuasa (pada waktu itu) adalah Kolonial Belanda yang jelas ingin mempertahankan dan mengokohkan kekuasaannya melalui berbagai undang-undang atau sistem hukumnya.

diajukan menjadi kebijaksanaan hakim, kecuali undang-undang menentukan lain. Sementara itu, sehubungan dengan bukti tertulis diatur dalam Pasal 183-188 BRV, dalam Pasal 186 BRV dinyatakan bahwa keabsahan tanda-tangan dapat dilakukan dengan apa saja.⁵⁹ Kedudukan hakim dalam hukum pembuktian Belanda ditantang untuk berperan dan mendalami persoalan-persoalan yang disengketakan. Dalam hal ini, tugas hakim harus melakukan pembagian beban pembuktian atas bukti-bukti yang diajukan para pihak.

Di Indonesia sendiri terdapat putusan pengadilan yaitu Putusan Mahkamah Agung Republik Indonesia (MARI) Nomor 9/KN/1999, yang dalam putusannya hakim menerima hasil *printout* sebagai alat bukti Surat. Kemudian kasus pidana yang diputus di Pengadilan Negeri Jakarta Timur mengetengahkan bukti *e-mail* (*electronic mailing*) sebagai salah satu alat bukti. Setelah mendengar keterangan ahli bahwa dalam transfer data melalui *e-mail* tersebut tidak terjadi tindakan manipulatif, hakim memvonis terdakwa dengan hukuman satu tahun penjara karena terbukti telah melakukan tindakan cabul berupa penyebaran tulisan dan gambar.⁶⁰ Hal ini merupakan perkembangan baru yang tepat untuk diikuti oleh hakim-hakim dalam memutus perkara *cyber*.

Kemudian peraturan perundang-undangan lain yang memberikan pengakuan terhadap dokumen elektronik adalah Undang-Undang Republik Indonesia Nomor 7 Tahun 1971 tentang Sistem Kearsipan yang menyatakan bahwa suatu informasi elektronik tetap diakui, karena definisi kearsipan tidak pernah menyatakan arsip

⁵⁹Isis lkhwansyah, *Op. Cit.*, h. 34.

⁶⁰Lihat, *Data Elektronik sebagai Alat Bukti Masih Dipertanyakan*, dalam http://www.hukumonline.com/artikel_detail.asp?id=8034. (Diakses pada tanggal, 26 Desember 2004).

harus dalam bentuk tertulis dalam media kertas saja tapi dimungkinkan juga untuk disimpan dalam media lainnya. Dalam undang-undang tersebut yang dimaksud dengan arsip ialah:

1. Naskah-naskah yang dibuat dan diterima oleh lembaga-lembaga negara dan badan-badan pemerintahan dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan tugas pemerintah.
2. Naskah-naskah yang dibuat dan diterima oleh badan-badan swasta dan/atau perorangan, dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan kehidupan kebangsaan.

Mengenai keamanan data, undang-undang ini mencantumkan ancaman pidana terhadap siapa saja yang melawan hukum dan/atau menyimpan dan dengan sengaja memberitahukan hal-hal tentang isi arsip tersebut kepada pihak ketiga yang tidak mengetahuinya.⁶¹

Dalam Undang-Undang ITE memuat hal yang baru mengenai data elektronik, yaitu dengan mengakui data elektronik yang terdapat pada ruang maya. Hal ini dapat dilihat pada BAB I mengenai Ketentuan Umum, Pasal 1 angka 4, yaitu:

Dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.⁶²

⁶¹Lihat, *Hukum dan Telematika: Kerangka Teknologi Informasi Nasional*, (Tim Koordinasi Telematika Indonesia, Februari, 2001).

⁶²Redaksi New Merah Putih, *Undang-Undang ITE (Informasi dan Transaksi Elektronik)* (Cet. I; Yogyakarta: New Merah Putih, 2009), h. 11.

Atas ketentuan tersebut, maka berkenaan dengan perspektif dokumen elektronik sebagai alat bukti pada *cyber crime* harus juga disertai dengan alat bukti lainnya sehingga sesuai dengan ketentuan alat bukti minimum dalam KUHAP. Selain itu keabsahan dokumen elektronik harus mendapatkan keyakinan dari hakim bahwa dokumen tersebut benar digunakan untuk melakukan *cyber crime*.

Melihat permasalahan hukum semakin pelik yang dihadapi penegak hukum saat ini adalah bagaimana menjaring pelaku kejahatan teknologi informasi yang mengusik rasa keadilan tersebut dikaitkan dengan ketentuan pidana yang berlaku. Hambatan yang ditemui oleh aparat penegak hukum adalah sulitnya menghukum si pelaku mengingat belum lengkapnya ketentuan pidana yang mengatur tentang kejahatan komputer, internet, dan teknologi informasi (*cyber crime*). Permasalahan utama adalah belum diterimanya dokumen elektronik (misalnya *file* komputer) sebagai alat bukti oleh konsep yang dianut KUHAP.⁶³

Mengingat kelemahan KUHAP tersebut, dalam menjalankan tugasnya penyidik harus dengan cerdik menggunakan definisi dokumen elektronik yang dapat diterima sebagai alat bukti. Pada dasarnya dalam praktik peradilan hakim sudah menerima dokumen elektronik sebagai alat bukti meskipun hal ini mungkin dilakukan tanpa sadar. Dalam kasus-kasus pidana yang berhubungan dengan perbankan, umumnya rekening koran atau dokumen apapun yang berisikan data nasabah berikut laporan keuangannya dihadirkan sebagai alat bukti surat. Padahal yang dimaksud dengan rekening koran sebenarnya adalah cetakan (*print out*) laporan

⁶³Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, *loc. cit.*, h. 36-38.

keuangan nasabah yang dalam bentuk aslinya berupa dokumen elektronik (*file* komputer).⁶⁴

Prosedur sistem perbankan modern saat ini seluruhnya menggunakan komputer sebagai petugas yang secara otomatis mendebet rekening nasabah (misalnya pengambilan lewat ATM atau pengambilan melalui cek dan giro) atau secara otomatis menambahkan bunga atas dana nasabah. Seluruh proses ini dicatat oleh komputer dan disimpan dalam bentuk *file*. Dengan demikian, Seluruh proses pembuktian kasus-kasus perbankan dalam kaitannya dengan dana nasabah sangatlah mustahil didasarkan pada dokumen yang aslinya berbentuk kertas. Kalaupun ada dokumen berbentuk kertas maka, itu hanyalah cetakan *file* komputer pada bank yang bersangkutan. Dengan diterimanya rekening koran tersebut sebagai alat bukti surat, maka hal ini dapat menjadi dasar bagi penyidik untuk menggunakan cetakan *file* komputer sebagai alat bukti surat.⁶⁵

Dalam transaksi elektronik yang berlangsung dengan menggunakan media elektronik, transaksi dilaksanakan tanpa tatap muka antara nasabah dengan petugas bank. Bukti atas transaksi yang dilakukan tersimpan dalam bentuk data elektronik yang terekam dalam sistem penyimpanan data di komputer. Mengenai alat-alat bukti

⁶⁴*Ibid.*

⁶⁵Budi Rahardjo dalam Draft Buku *Cyber Law “Pernak Pernik Peraturan dan Pengaturan Cyber Space di Indonesia”* menyatakan bahwa sebuah berkas elektronik (*electronic file*), seperti misalnya sebuah *e-mail*, dapat dijadikan bukti ataupun tidak dapat. Pihak yang berpendapat bahwa digital *file* tidak dapat dijadikan bukti mengatakan bahwa *file* dapat dibuat dengan mudah. Bisa saja seseorang (bahkan mungkin juga penyidik) yang membuat atau mengubah file tersebut, bukan tertuduh. Memang benar *file* digital mudah dibuat dan diubah. Akan tetapi ada jejak-jejak yang dibuat ketika kita membuat sebuah berkas digital. Tergantung kepada sistem operasi komputer yang digunakan, sistem komputer mencatat perubahan yang dilakukan terhadap sistem (termasuk membuat *file*) dalam berbagai berkas. Biasanya ini dikenal dengan istilah “log”. Selain log, ada juga tanda-tanda lain yang melekat pada berkas itu sendiri (kapan berkas dibuat, kapan terakhir diakses) atau tercatat di *file system* (misalnya di *File Allocation Table*, FAT).

dalam transaksi elektronik, Michael Chissick dan Alistair Kelman menyatakan ada tiga tipe pembuktian yang dibuat oleh komputer, yaitu:

1. *Real Evidence* (bukti nyata)

Real evidence atau bukti nyata ini meliputi kalkulasi-kalkulasi atau analisa-analisa yang dibuat oleh komputer itu sendiri melalui pengaplikasian *software* dan penerima informasi dari *device* lain seperti jam yang *built-in* langsung dalam komputer atau *remote sender*. Bukti nyata ini muncul dari berbagai kondisi. Jika sebuah komputer bank secara otomatis mengalkulasi (menghitung) nilai pembayaran pelanggan terhadap bank berdasarkan tarifnya, transaksi-transaksi yang terjadi dan *credit balance* yang dikliring secara harian, maka kalkulasi ini akan digunakan sebagai sebuah bukti nyata.

2. *Hearsay Evidence* (bukti yang berupa kabar dari orang lain)

Termasuk pada *hearsay evidence* adalah dokumen-dokumen data yang diproduksi oleh komputer yang merupakan salinan dari informasi yang diberikan (dimasukkan) oleh manusia kepada komputer. Cek yang ditulis dan slip pembayaran yang diambil dari sebuah rekening bank juga termasuk *hearsay evidence*.

3. *Derived Evidence*

Yang dimaksud dengan *derived evidence* adalah informasi yang mengkombinasikan antara bukti nyata (*real evidence*) dengan informasi yang diberikan oleh manusia ke komputer dengan tujuan untuk membentuk sebuah data yang tergabung. Contoh dari *derived evidence* adalah tabel dalam kolom-kolom harian sebuah *statement* bank karena tabel ini adalah diperoleh dari *real evidence*

(yang secara otomatis membuat tagihan bank) dan *hearsay evidence* (*check* individu dan *entry* pembayaran lewat *slip-paying in*).⁶⁶

Menurut Budi Rahardjo, banyak orang yang beranggapan bahwa jika belum ada *cyber law* maka kita vakum hukum sehingga kejahatan di dunia maya dapat dilakukan. Ini adalah anggapan yang salah. Lebih lanjut dinyatakan bahwa para penegak hukum dapat menggunakan hukum-hukum yang berlaku/konvensional untuk menjerat para pelaku *cyber crime* meskipun KUHAP sebagai landasan hukum konvensional akan mempersulit pekerjaan penegak hukum.⁶⁷

Mengenai pembuktian isi berkas atau dokumen itu sendiri memang tidak mudah dibuktikan. Sifat yang ingin dibuktikan adalah sifat *integrity*. Sifat ini dapat terjaga dan dibuktikan jika digunakan *digital signature* untuk mengesahkan berkas tersebut. Dengan *digital signature*, perubahan satu huruf saja dalam isi berkas akan dapat ditunjukkan bahwa berkas sudah berubah (meskipun tidak ditunjukkan apanya yang berubah). Tanpa *digital signature* akan sulit melakukan pembuktian. Namun ini bukan berarti tidak mungkin, hanya sangat sulit.⁶⁸

Kesulitan selama ini dapat diatasi dengan menambahkan data elektronik dalam Pasal 184 KUHAP sebagai alat bukti yang sah. Perbaikan KUHAP atas pasal tersebut merupakan salah satu cara untuk menghadapi *cyber crime*. Onno W. Purbo menyatakan, sudah saatnya pemerintah memperbaiki KUHAP dengan menempatkan

⁶⁶Michael Chissick dan Akistair Kelman, *Electronic Commerce Law Practic* sebagaimana dikutip dari M. Arsyad Sanusi, *E-Commerce: Hukum dan Solusiny*, (Bandung: PT. Mizan Grafika Sarana, 2001), h. 97-98.

⁶⁷Budi Rahardjo, *loc. cit.*

⁶⁸Dalam Rancangan Undang-Undang Teknologi Informasi, *digital signature* ditentukan dalam Pasal 1 angka 8 yang menyatakan: “*sertifikat tanda tangan adalah sertifikat yang dikeluarkan oleh lembaga sertifikasi tanda tangan digital berdasarkan ketentuan yang berlaku.*”

data elektronik sebagai alat bukti yang sah di pengadilan. KUHAP harus mengakui data elektronik sebagai alat bukti yang sah untuk mengungkap kasus kejahatan internet. Selanjutnya menurut Onno, pekerjaan itu memang bukan hal yang mudah dan butuh waktu. Dengan memberi masukan pada KUHAP, khususnya Pasal 184 diharapkan kejahatan *cyber* dapat dibendung dan pelaku kejahatan *cyber* dapat dijerat dengan alat bukti digital yang sah.⁶⁹

Dalam kasus *cyber crime*, proses penegakan hukum tidak dapat begitu saja dilepaskan dengan dalih kesulitan pada proses pembuktian. Apalagi jika terhadap perbuatan *cyber crime* tersebut telah dapat dikenakan delik-delik konvensional yang ketentuannya jelas dan tegas. Upaya yang dapat ditempuh adalah penelusuran bukti-bukti yang berkaitan dengan perbuatan pelaku *cyber crime* melalui jalur KUHAP. Artinya, di sini kita tetap menggunakan alat-alat bukti berupa keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Minimalnya, kesalahan pelaku dapat terbukti dengan sekurang-kurangnya 2 (dua) alat bukti yang sah.⁷⁰ Alat-alat bukti ini harus mampu membuktikan telah terjadi suatu perbuatan dan membuktikan adanya akibat dari perbuatan *cyber crime*.

1. Keterangan Saksi

Berkenaan dengan sifat *cyber crime* yang virtual, maka pembuktian dengan menggunakan keterangan saksi tidak dapat diperoleh secara langsung. Keterangan saksi hanya dapat berupa hasil pembicaraan atau hanya mendengar dari orang lain. Kesaksian ini dikenal sebagai *testimonium de auditum* atau *hearsay evidence*. Meskipun kesaksian sejenis ini tidak diperkenankan sebagai alat bukti, akan tetapi

⁶⁹Onno W. Purbo, “Hadapi Kejahatan Internet, KUHAP Perlu Disempurnakan”, dalam <http://www.hukum.online> (Diakses pada tanggal, 27 April 2005).

⁷⁰Pasal 183 KUHAP.

dalam praktiknya tetap dapat dipergunakan sebagai bahan pertimbangan bagi hakim untuk memperkuat keyakinannya sebelum menjatuhkan putusan.⁷¹

Kemungkinan yang dapat dijadikan keterangan saksi ialah melalui hasil interaksi di dalam dunia *cyber*, seperti *chatting* dan *e-mail* antara pengguna internet, atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi.⁷²

2. Keterangan Ahli

Keterangan ahli menjadi signifikan penggunaannya jika jaksa mengajukan alat bukti elektronik untuk membuktikan kesalahan pelaku *cyber crime*. Peran keterangan ahli di sini adalah untuk memberikan suatu penjelasan di dalam persidangan bahwa dokumen/data elektronik yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum. Hal ini diperlukan karena terkadang dalam praktiknya, para pelaku *cyber crime* dapat menghapus atau menyembunyikan aksi mereka agar tidak terdeteksi oleh aparat penegak hukum.

Saksi ahli ini tidak terbatas hanya pada operator laboratorium forensik komunikasi, lebih luas lagi melibatkan ahli-ahli dalam berbagai bidang antara lain ahli dalam teknologi informasi, mendesain internet, program-program jaringan komputer serta ahli dalam bidang enkripsi/*password* atau pengamanan jaringan komputer. Kombinasi dari fakta-fakta yang didapat dari laboratorium forensik dan opini para saksi ahli diharapkan dapat membantu para penyidik dalam proses

⁷¹Pada umumnya alat bukti keterangan saksi merupakan alat bukti yang paling utama dalam perkara pidana. Secara umum, setiap perkara pidana menggunakan alat bukti keterangan saksi dalam pembuktiannya. Sekurang-kurangnya, di samping pembuktian dengan alat bukti yang lain, pembuktian dengan alat bukti keterangan saksi masih tetap diperlukan.

⁷²Berdasarkan Pasal 1 butir 26 KUHP, Pengguna internet dan Pegawai administrator sistem komputer telah memenuhi syarat sebagai seorang saksi.

penyidikan, dimana produk hasil penyidikan tersebut dapat diterima oleh jaksa penuntut umum dan hakim.

Peranan seorang ahli dalam *cyber crime* merupakan sesuatu yang tidak bisa ditawar-tawar lagi mengingat pembuktian dengan alat bukti elektronik masih sangat riskan penggunaannya di depan sidang pengadilan. Di sinilah pentingnya kedudukan seorang ahli, yaitu untuk memberikan keyakinan kepada hakim.

3. Alat Bukti Surat

Surat adalah alat bukti yang penting dalam proses penyelidikan dan penyidikan kasus *cyber crime*. Penyelidik dan penyidik dapat menggunakan “surat” untuk membuat terang kasus ini. Dengan didukung oleh keterangan saksi, maka surat menjadi alat bukti yang sah, dapat diterima dan dapat memberatkan pelaku kasus *cyber crime* di pengadilan.

Merujuk pada terminologinya,⁷³ “Surat” dalam kasus *cyber crime* mengalami perubahan dari bentuknya yang tertulis menjadi tidak tertulis dan bersifat *on-line*. Alat bukti surat dalam sistem komputer yang telah disertifikasi ada dua kategori.⁷⁴ *Pertama*, bila sebuah sistem komputer yang telah disertifikasi oleh badan yang

⁷³Alat bukti Surat dirumuskan dalam Pasal 187 KUHAP yang berisi:

“Surat sebagaimana tersebut pada pasal 184 ayat 1 huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, adalah:

- a. berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat di hadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau yang dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu;
- b. surat yang dibuat menurut ketentuan peraturan perundang-undangan atau Surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan;
- c. surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi dari padanya;
- d. surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.”

⁷⁴Edmon Makarim, *op. cit.*, h. 437.

berwenang, maka hasil *print out* komputer dapat dipercaya keotentikannya. Contohnya *receipt* yang dikeluarkan oleh suatu bank dalam transaksi ATM. Alat bukti ini mempunyai kekuatan pembuktian meskipun dalam persidangan akan dibutuhkan keterangan lebih lanjut.

Kedua, bukti sertifikasi dari badan yang berwenang tersebut dapat di kategorikan sebagai alat bukti surat, karena dibuat oleh dan atau pejabat yang berwenang. Meskipun penggunaan kedua bukti surat ini mengalami kendala dari segi pengertian “pejabat yang berwenang” di mana di dalam perundang-undangan yang dimaksud dengan pejabat yang berwenang adalah notaris.

Jenis alat bukti surat lainnya dapat berupa bukti elektronik yang dapat dicetak atau *print out* dan surat yang terpampang dalam layar monitor sebuah jaringan komputer. Selama kedua bukti ini dikeluarkan/dibuat oleh yang berwenang dan sebuah sistem jaringan komputer tersebut dapat dipercaya, maka surat tersebut memiliki kekuatan pembuktian yang sama dengan alat bukti surat sebagaimana yang ditentukan dalam KUHAP.

4. Petunjuk

Berdasarkan Pasal 188 KUHAP, petunjuk adalah perbuatan, kejadian atau keadaan, yang karena persesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya. Petunjuk tersebut hanya dapat diperoleh dari keterangan saksi, surat dan keterangan terdakwa yang penilaian atas kekuatan pembuktiannya dalam setiap keadaan tertentu dilakukan oleh hakim dengan arif lagi bijaksana, setelah hakim mengadakan pemeriksaan dengan penuh kecermatan dan keseksamaan berdasarkan hati nuraninya.

Dalam *cyber crime*, pengumpulan alat bukti secara fisik akan sulit dipenuhi. Yang paling mudah dalam melakukan pengumpulan bukti-bukti adalah mencari petunjuk-petunjuk yang mengindikasikan telah adanya suatu niat jahat berupa akses secara tidak sah. Misalnya dengan melihat dan mendengarkan keterangan saksi di pengadilan, atau surat elektronik atau hasil *print out* data, atau juga dari keterangan terdakwa di pengadilan.

Mewujudkan suatu petunjuk dari bukti-bukti yang ditemukan dalam *cyber crime* akan sulit jika hanya didasarkan pada keterangan saksi, surat, keterangan terdakwa saja meskipun hal tersebut masih mungkin untuk diterapkan.⁷⁵ Bisa saja hakim memperoleh petunjuk dari alat-alat bukti tersebut di persidangan. Akan tetapi apabila hakim memperoleh petunjuk yang diajukan di persidangan adalah bukti elektronik (yang disertai dengan keterangan ahli), maka petunjuk ini akan bersifat lebih kuat dan memberatkan terdakwa dibandingkan dengan petunjuk-petunjuk lain.

5. Keterangan Terdakwa

Dalam Pasal 189 ayat 1 KUHAP ditentukan bahwa keterangan terdakwa adalah apa yang terdakwa lakukan, ketahui dan alami sendiri. Dalam kasus *cyber crime*, keterangan terdakwa yang dibutuhkan terutama mengenai cara-cara pelaku melakukan perbuatannya, akibat yang ditimbulkan, informasi jaringan serta motivasinya. Keterangan terdakwa mengenai keempat hal tersebut sifatnya adalah memberatkan terdakwa.

Pada praktiknya, perolehan keterangan terdakwa menjadi sesuatu proses yang sulit dilakukan. Hal ini dikarenakan, kemampuan/pengetahuan teknologi informasi

⁷⁵*Ibid.*, h. 443.

penyidik yang terbatas, pelaku *cyber crime* yang sulit untuk diidentifikasi secara pasti, serta kuatnya jaringan di antara sesama pelaku *cyber crime*.

Meskipun bukan tidak mungkin dapat dilakukan penangkapan dan penahanan terhadapnya, keterangan terdakwa yang bersifat memberatkan akan sulit diperoleh mengingat seorang pelaku *cyber crime* tidak akan bersedia membocorkan atau membuka rahasia jaringan/kelompok, baik rahasia identitas pelaku lain maupun rahasia cara kerjanya. Jika keterangan terdakwa dapat diajukan ke pengadilan dan hakim menilai bahwa keterangan tersebut adalah sah. Kemudian atasnya hakim memperoleh keyakinan, maka terhadap terdakwa pelaku *cyber crime* tersebut dapat dikenakan delik-delik KUHP.

Dalam penggunaan alat-alat bukti konvensional atas kejahatan *cyber*, hakim memegang peranan penting dalam penyelesaian perkara dengan wajib menggali hukum yang hidup dalam masyarakat. Hakim harus, membuat terobosan hukum jika belum ada undang-undang yang mengaturnya. Keyakinan hakim untuk menerima alat bukti di persidangan menjadi hal yang signifikan adanya. Demikian pentingnya peran hakim dalam kasus *cyber crime*, hakim harus mempunyai kemampuan dalam ilmu teknologi informasi dan pandangan yang luas dalam penafsiran hukum.

Hal tersebut di atas menunjukkan bahwa penggunaan sistem pembuktian dan alat-alat bukti berdasarkan pasal 184 KUHP mampu menjangkau pembuktian untuk kejahatan *cyber* yang tergolong tindak pidana baru. Penelusuran terhadap alat-alat bukti konvensional seperti keterangan saksi dan saksi ahli, juga pergeseran surat dan petunjuk dari konvensional menuju elektronik akan mampu menjerat pelaku *cyber crime*.

Hal ini tentu saja membutuhkan kecermatan para penegak hukum dalam menggunakannya untuk kemudian dapat diajukan dan diterima oleh hakim. Lebih lanjut, tidak terlepas dari sifatnya sebagai tindak pidana baru, maka kejahatan *cyber* atau *cyber crime* ini pada akhirnya undang-undang baru yang mendukung seluruh perangkat hukum. Undang-Undang ITE melahirkan ketentuan baru yakni diterimanya alat bukti elektronik dapat diterima sebagai alat bukti yang sah di depan persidangan. Dengan ini harapannya aparat penegak hukum tidak lagi menemukan kesulitan dalam menjerat para pelaku kejahatan di dunia *cyber* yang dinilai meresahkan masyarakat.

G. Sanksi Pidana Bagi Pelaku Cyber Crime

Dalam sejarah perkembangan hukum pidana dapat diungkapkan adanya 3 macam teori yang mengemukakan tujuan pemidanaan, yaitu teori absolut (*vergelding theorien*), teori relatif (*doel theorien*), dan teori gabungan (*vernengings theorien*).⁷⁶ Teori tersebut mengkaji tentang alasan pembenaran penjatuhan pidana.

Menurut teori absolut, pidana sama sekali tidak mengandung pertimbangan tujuan dan manfaat bagi terpidana. Pidana hanya dimaksudkan untuk memberikan nestapa guna memberi imbalan agar tercipta ketertiban hukum.⁷⁷ Dasar pijakan teori absolut dalam penjatuhan pidana adalah pada aspek pembalasan yang setimpal pada penjahat, karena itu teori ini disebut juga teori pembalasan. Siapa saja berbuat jahat harus dipidana tanpa melihat akibat-akibat apa saja yang timbul setelah

⁷⁶Adami Chazawi, *Pelajaran Hukum Pidana (Bagian I)*, (Malang: Biro Konsultasi dan Bantuan Hukum Fakultas Hukum Universitas Brawijaya, 2001), h. 170.

⁷⁷J. J. M. Van Dijk , et all., *Actuele Criminologie* diterjemahkan oleh Soemitro (Surakarta: Universitas Sebelas Maret Press, 1996), h. 218.

penjatuhannya pidana, baik terhadap terpidana maupun masyarakat. Faktor yang dipertimbangkan hanya masa lalu terpidana, tidak melihat masa depan terpidana. Tujuan pemidanaan adalah menjadikan si penjahat menderita, dengan jalan menjatuhkan pidana sebagai pembalasan.⁷⁸ Pembalasan tersebut dipandang sebagai suatu reaksi keras yang bersifat emosional, karena itu mempunyai sifat yang irasional.⁷⁹

Dengan demikian teori absolut dapat disimpulkan bahwa menurut teori absolut, pidana dijatuhkan oleh negara kepada siapa saja yang melakukan kejahatan yang setimpal dengan perbuatannya. Pidana dijatuhkan semata berdasarkan pembalasan atas perbuatannya. Pidana tidak diorientasikan pada masa depan nara pidana, tetapi didasarkan pada masa lalu penjahat. Tujuan pidana adalah menjadikan penjahat menderita.

Dalam perkembangan pemikiran pemidanaan selanjutnya lahir teori relatif atau lazim disebut teori tujuan atau teori prevensi. Teori tujuan ini bukan merupakan penyempurnaan atau perbaikan atas ketidakberhasilan teori pembalasan. Dalam teori relatif, tujuan pidana diarahkan pada usaha agar kejahatan yang telah dilakukan oleh penjahat tidak terulang lagi. Pejatuhannya pidana bukan hanya memperhatikan masa lalu penjahat, tetapi juga memperhatikan masa depannya. Teori prevensi melihat pada sifat berbahaya pribadi si pelaku kejahatan, dan terhadap mereka yang mempunyai kecenderungan untuk melakukan perbuatan jahat, karena itu dalam teori ini dikenal istilah prevensi khusus dan prevensi umum. Teori-teori relatif, baik teori prevensi umum (misalnya yang dikemukakan oleh Seneca) maupun teori prevensi

⁷⁸Made Shadi Astuti, *Pemidanaan Terhadap Anak sebagai Pelaku Tindak Pidana* (Malang: IKIP Malang), h. 27.

⁷⁹J. E. Sahetapy, *Kriminologi* (Jakarta: Rajawali, 1998), h. 11.

khusus (misalnya yang didukung oleh Van Hammel), tidak memandang penjatuhan pidana sebagai suatu konsekuensi atas kesalahan yang sudah dilakukan oleh seseorang pada masa lalu, melainkan untuk mencegah terulangnya kejahatan. Teori prevensi menganggap bahwa kesalahan seseorang berada di luar perhatiannya. Pidana merupakan sarana untuk mencegah kejahatan di masa mendatang. Perbuatan manusia bukan menjadi dasar hukum atau alasan untuk menjatuhkan pidana, melainkan hanya dianggap sebagai keadaan yang menimbulkan pidana. Tindak pidana merupakan petunjuk tentang adanya keadaan bahaya untuk itu negara harus melakukan reaksi berupa penjatuhan pidana.

Melihat teori tersebut di atas, terlihat bahwa tindak pidana dibebankan kepada pelaku kejahatan berdasarkan tingkat kejahatan yang dilakukannya. Hal ini terlihat dalam sanksi pidana dalam kejahatan *cyber crime* dalam undang-undang yang berlaku sebagaimana disebutkan dalam Undang-Undang ITE. Berikut ini di paparkan jenis kejahatan dan ancamannya:⁸⁰

1. Penipuan

Rumusan tindak pidana penipuan dalam dunia *cyber* pada dasarnya merujuk pada tindak pidana umum. Tindak pidana sebagaimana diatur dalam pasal 378 KUHP disebut tindak pidana penipuan dalam bentuk pokok yang lazim disebut "*oplichting*". Ketentuan pasal tersebut menyatakan:

Barang siapa yang bermaksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, atau rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan sesuatu barang kepadanya, atau supaya memberi hutang

⁸⁰Lihat, Redaksi New Merah Putih, *op. cit.*

maupun menghapus piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun.⁸¹

Berdasarkan ketentuan pasal tersebut, maka tindak pidana penipuan (dalam bentuk pokok) mempunyai unsur-unsur sebagai berikut:

a. Unsur-unsur obyektif, yang terdiri dari:

- 1) Menggerakkan,
- 2) Orang lain,
- 3) Untuk menyerahkan barang/benda,
- 4) Untuk memberi hutang,
- 5) Untuk menghapus piutang,
- 6) Dengan menggunakan daya upaya seperti:
 - a) Memakai nama atau,
 - b) Martabat palsu,
 - c) Dengan tipu muslihat, dan
 - d) Rangkaian kebohongan.

b. Unsur-unsur subyektif, yang terdiri dari:

- 1) Dengan maksud,
- 2) Untuk menguntungkan diri sendiri atau orang lain, dan
- 3) Secara melawan hukum.

Mencermati rumusan dalam pasal tersebut, tindak pidana penipuan sebagaimana dirumuskan dalam Undang-Undang ITE pada Pasal 28 Ayat (1) juga menyiratkan esensi sebuah tindak pidana penipuan, hanya dalam pasal tersebut

⁸¹Hari Sasangka dan Ahmad Rifai, *KUHP (Kitab Undang-Undang Hukum Pidana) Disertai Yurisprudensi Mahkamah Agung Republik Indonesia* (Cet. I; Bandung: CV. Mandar Maju, 2010), h. 161.

dilakukan melalui transaksi elektronik. Hal ini dapat dilihat dalam Undang-Undang ITE pada Pasal 28 Ayat (1) disebutkan bahwa:

Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Adapun sanksi dari tindak pidana tersebut dapat dilihat pada Pasal 45 Ayat (2) sebagai berikut:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

2. Kesusilaan

Kejahatan terhadap kesusilaan, khususnya terhadap tindak pidana pornografi sebagaimana diatur dalam KUHP Pasal 282 dan 283. Pasal tersebut yang menjadi landasan pokok terhadap kejahatan kesusilaan dalam kejahatan *cyber crime*. Dalam Undang-Undang ITE pada Pasal 27 Ayat (1) sebagai berikut:

Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

Adapun sanksi pidananya diatur dalam Pasal 45 Ayat (1) sebagai berikut:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

3. Perjudian

Tindak pidana ini diatur dalam Pasal 303 KUHP dan Pasal 303 bis KUHP jo. Undang-Undang Republik Indonesia Nomor 7 Tahun 1974 yang mengubah sanksinya. Oleh karena itu, sanksi pidana yang semula hukuman penjara selamalamanya dua tahun delapan bulan atau denda sebanyak-banyaknya sembilan puluh

ribu rupiah menjadi hukuman selama-lamanya sepuluh tahun atau denda sebanyak-banyaknya dua puluh lima juta rupiah.

Dalam dunia *cyber*, tindak pidana ini telah diatur dalam Pasal 27 Ayat (2) sebagaiberikut:

Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

Adapun sanksi pidananya telah diatur dalam Pasal 45 Ayat (1) sebagai berikut:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

Jika tindakan ini dilakukan secara berkelompok atau korporasi, maka Pasal 52 Ayat (4) mengatur pula:

Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

4. Pemerasan/Pengancaman

Tindak pidana pemerasan dan pengancaman sebagaimana diatur dalam Pasal 368 dan 369 KUHP sama-sama merupakan pemerasan. Perbedaannya hanya terletak pada cara-cara yang digunakan dalam kedua tindak pidana tersebut. Tindak pidana dalam Pasal 368 KUHP yang lazim disebut “pemerasan” menggunakan “kekerasan atau ancaman kekerasan” sedangkan tindak pidana dalam Pasal 369 KUHP yang lazim disebut sebagai “pengancaman” menggunakan cara “pencemaran baik lisan maupun tertulis”.

Dalam ketentuan Pasal 368 KUHP tindak pidana pemerasan dirumuskan sebagai berikut:

- 1) Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang lain dengan kekerasan atau ancaman kekerasan, untuk memberikan sesuatu barang, yang seluruhnya atau sebagian adalah milik orang lain, atau supaya memberikan hutang maupun menghapus piutang, diancam, karena pemerasan dengan pidana penjara paling lama sembilan tahun.
- 2) Ketentuan Pasal 365 ayat (2), ayat (3), dan ayat (4) berlaku dalam tindak pidana ini.

Melihat unsur-unsur yang ada di dalam ketentuan Pasal 365 KUHP tersebut untuk melihat perbuatan apa yang dirumuskan dalam pasal ini, adalah sebagai berikut:

- a) Unsur obyektif, yang meliputi unsur-unsur:
 - (1) Memaksa,
 - (2) Orang lain,
 - (3) Dengan kekerasan atau ancaman kekerasan,
 - (4) Untuk memberikan atau menyerahkan sesuatu barang (yang seluruhnya atau sebagian orang lain),
 - (5) Supaya memberi utang, dan
 - (6) Untuk menghapus piutang.
- b) Unsur subyektif, yang meliputi unsur-unsur:
 - (1) Dengan maksud, dan
 - (2) Untuk menguntungkan diri sendiri atau orang lain.

Sedangkan dalam ketentuan pasal 369 KUHP dinyatakan sebagai berikut:

- 1) Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancaman pencemaran baik lisan maupun tulisan atau dengan ancaman akan membuka rahasia, memaksa seseorang supaya memberikan sesuatu barang yang seluruhnya atau

sebagian milik orang lain itu atau orang lain, atau supaya memberikan hutang atau menghapus piutang, diancam dengan pidana penjara paling lama empat tahun.

- 2) Kejahatan ini tidak dituntut kecuali atas pengaduan orang yang terkena kejahatan.

Melihat unsur-unsur Pasal 368 dan 369 KUHP terlihat dengan jelas, bahwa bangunan hukum antara kedua tindak pidana tersebut memiliki esensi yang sama, yaitu memeras orang lain. Hanya kedua tindak pidana tersebut menggunakan cara-cara yang berbeda untuk mencapai maksudnya.

Kedua pasal tersebut menjadi rujukan dalam penerapan tindak pidana *cyber crime* yang terbagun dan terumus dalam rumusan dalam Pasal 27 Ayat (4) sebagai berikut:

Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Adapun sanksi pidana terhadap tindak pidana tersebut telah diatur sebagaimana diatur dalam Pasal 45 Ayat (1) sebagai berikut:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

Apabila dilakukan secara berkelompok atau terorganisir akan di kenai sanksi sesuai Pasal 52 Ayat (4):

Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

Berkaitan dengan tindak pidana pengancaman yang disertai dengan ancaman kekerasan Undang-Undang ITE dalam Pasal 29 menyatakan:

Setiap orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah).

5. Pengerusakan

Tindak pidana ini dalam KUHP telah diatur ketentuannya dalam Pasal 406 yang menyatakan:

- (1) Barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tidak dapat dipakai atau menghilangkan sesuatu barang yang seluruhnya atau sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah.
- (2) Dijatuhkan pidana yang sama terhadap orang, yang dengan sengaja dan melawan hukum membunuh, merusakkan, membikin tak dapat digunakan atau menghilangkan hewan, yang seluruhnya atau sebagian milik orang lain.

Apabila unsur-unsur dalam tindak pidana tersebut diuraikan secara terperinci, maka unsur-unsur dalam tindak pidana tersebut adalah sebagai berikut:

a. Unsur-unsur pidana Pasal 406 ayat (1) KUHP

1) Unsur-unsur obyektif, yang meliputi:

- a) Menghancurkan, merusak, membuat tidak dapat dipakai atau menghilangkan,
- b) Suatu barang, dan
- c) Yang seluruh atau sebagian milik orang lain.

2) Unsur-unsur subyektif, yang meliputi:

- a) Dengan sengaja, dan
- b) melawan hukum.

b. Unsur-unsur pidana Pasal 406 ayat (2) KUHP:

1) Unsur-unsur obyektif, yang meliputi:

- a) Menghancurkan, merusak, membuat tidak dapat dipakai atau menghilangkan,
 - b) Seekor hewan, dan
 - c) Yang seluruh atau sebagian milik orang lain.
- 2) Unsur-unsur subyektif, yang meliputi:
- a) Dengan sengaja, dan
 - b) melawan hukum.

Melihat unsur-unsur yang ada dalam undang-undang tersebut, tindak pidana pengerusakan dalam *cyber crime* sebagaimana diatur dalam Undang-Undang ITE terlihat sama, karena unsur-unsur tersebut menjadi ketentuan dalam rumusan suatu tindak pidana pengerusakan. Hal ini, apabila unsur-unsurnya terpenuhi maka akan dipidana sesuai dengan ketentuan perundang-undang yang berlaku. Hal ini dapat dilihat dalam Pasal 33 sebagai berikut:

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah).

6. Pencurian

Dalam Kitab Undang-Undang Hukum Pidana (KUHP) Pasal 362 dinyatakan bahwa:

Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau denda paling banyak sembilan ratus rupiah.⁸²

⁸²Hari Sasangka dan Ahmad Rifai, *op. cit.*, h. 151.

Jika diteliti rumusan tindak pidana pencurian tersebut, maka perbuatan itu memiliki beberapa unsur-unsur, yaitu:

1. Barang siapa,
2. Mengambil sesuatu barang,
3. Barang kepunyaan/milik orang lain,
4. Dengan maksud untuk dimiliki secara melawan hukum.

Untuk diketahui bahwa Pasal 362 KUHP itu terdiri atas 4 unsur seperti tersebut tanpa menitik beratkan satu unsur. Masing-masing unsur mengandung arti yuridis untuk dipakai menentukan atas suatu perbuatan.

Terkait dengan hal tersebut, bahwa tindak pidana konvensional dengan tindak pidana *cyber crime* pada dasarnya memiliki kesamaan. Hanya yang membedakan unsur-unsur pidana dalam dunia *cyber crime* pada modus operandi.

Dalam Undang-Undang ITE pada Pasal 30 Ayat (1), (2) dan (3) disebutkan bahwa:

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
- (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 46 Ayat (1), (2) dan (3) disebutkan:

- (1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

- (2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).
- (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Sedangkan Pasal 52 Ayat (2) dan (3) dinyatakan pula:

- (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap komputer dan/atau sistem elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik pemerintah dan/ atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.
- (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap komputer dan/atau sistem elektronik serta Informasi Elektronik dan/ atau Dokumen Elektronik milik pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank central, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing pasal ditambah dua pertiga.

Mencermati Undang-Undang ITE pada Pasal 30 Ayat (1), (2) dan (3) terlihat adanya kesamaan unsur-unsur tindak pidana. Dalam dunia *cyber crime* yang membedakan hanya modus operandi dan di dalam dunia yang berbeda yakni dunia *cyber*. Oleh karena itu, pelaku pencurian dalam dunia *cyber* akan dipidana sebagaimana diatur pada Pasal 46 Ayat (1), (2) dan (3) dan Pasal 52 Ayat (2) dan (3).

BAB IV

MENCARI AKAR *CYBER CRIME* DALAM ISLAM

A. Perspektif Hukum Pidana Islam tentang Cyber Crime

Hukum pidana Islam merupakan syariat Allah swt. yang mengandung kemaslahatan dalam kehidupan manusia di dunia dan di akhirat. Syariat dimaksud, secara materiil mengandung kewajiban asasi bagi setiap manusia untuk melaksanakannya. Konsep kewajiban asasi syariat, yaitu menempatkan Allah swt. sebagai pemegang segala hak, baik yang ada pada diri sendiri maupun yang ada pada orang lain. Setiap orang hanya sebagai pelaksana yang berkewajiban memenuhi perintah Allah swt. Perintah Allah dimaksud, harus ditunaikan untuk kemaslahatan dirinya dan orang lain.¹

Alquran merupakan penjelasan Allah swt. tentang syariat, sehingga disebut *al-Bayan* (penjelasan). Penjelasan dimaksud secara garis besar mempunyai empat cara dan salah satunya adalah Allah swt. memberikan penjelasan dalam bentuk *nash* (tekstual) tentang sesuatu syariat, misalnya: orang yang mengambil barang milik orang lain di tempat penyimpanan dengan cara yang tidak benar yang melebihi batas nisabnya harus dipotong tangannya atas adanya putusan dari pengadilan.²

Kalau ditelusuri lebih jauh Allah membatasi tingkah laku manusia melalui syariatnya semata-mata karena ingin menegakkan keadilan, kedamaian, ketertiban dan ketentraman masyarakat. Sehingga apabila syariat itu dapat ditegakkan sudah pasti tujuan hidup dapatlah dicapai. Hal ini dimaksudkan agar tujuan syariat dapat

¹Zainuddin Ali, *Hukum Islam: Pengantar Ilmu Hukum Islam di Indonesia* (Jakarta: Sinar Grafika, 2008), h. 102.

²*Ibid.*

terwujud yakni, terpeliharanya agama, jiwa, keturunan atau kehormatan, harta dan akal. Mengapa hal ini perlu diwujudkan? Karena semata-mata ingin menjaga manusia dari kesempurnaan yang diberikan oleh Allah swt.

Berkaitan dengan hal tersebut, asas universal juga menyebutkan bahwa memelihara ketertiban umum di atas kepentingan pribadi merupakan suatu keharusan dan kewajiban bagi setiap manusia. Oleh karena itu, tindakan yang bertentangan dengan asas tersebut dinilai sebagai suatu pelanggaran hukum. Misalnya, membuat keonaran, keributan dan perusakan di lingkungan masyarakat tentu mengganggu masyarakat yang lainnya. Asas tersebut sejalan dengan Alquran dalam Q.S. Al-Maidah/5: 64 sebagai berikut:

وَقَالَتِ الْيَهُودُ يَدُ اللَّهِ مَغْلُولَةٌ ۖ غُلَّتْ أَيْدِيهِمْ وَلُعِنُوا بِمَا قَالُوا ۖ بَلْ يَدَاهُ مَبْسُوطَتَانِ يُنفِقُ
كَيْفَ يَشَاءُ ۚ وَلَيَزِيدَنَّ كَثِيرًا مِّنْهُمْ مَا أُنْزِلَ إِلَيْكَ مِنْ رَبِّكَ طُغْيَانًا وَكُفْرًا ۚ وَأَلْقَيْنَا بَيْنَهُمُ
الْعَدَاوَةَ وَالْبَغْضَاءَ إِلَى يَوْمِ الْقِيَامَةِ ۚ كُلَّمَا أَوْقَدُوا نَارًا لِلْحَرْبِ أَطْفَأَهَا اللَّهُ ۚ وَيَسْعَوْنَ فِي
الْأَرْضِ فَسَادًا ۚ وَاللَّهُ لَا يُحِبُّ الْمُفْسِدِينَ

Terjemahnya:

Dan Orang-orang Yahudi berkata: “Tangan Allah terbelenggu”. Sebenarnya tangan merekalah yang dibelenggu dan merekalah yang dilaknat disebabkan apa yang telah mereka katakan itu. Padahal kedua tangan Allah terbuka; Dia memberi rezki sebagaimana dia kehendaki. Dan (Alquran) yang diturunkan kepadamu dari Tuhanmu itu pasti akan menambah kedurhakaan dan kekafiran bagi kebanyakan mereka. Dan Kami timbulkan permusuhan dan kebencian di antara mereka sampai hari kiamat. Setiap mereka menyalakan api peperangan, Allah memadamkannya dan mereka berbuat kerusakan dimuka bumi dan Allah tidak menyukai orang-orang yang membuat kerusakan.³

³Departemen Agama RI, *Alquran dan Terjemahnya* (Cet. X; Bandung: PT. Syamil Cipta Media, 2006), h. 118.

Dalam surat yang lain juga dinyatakan (Q.S. Al-Baqarah/2: 205) sebagai berikut:

وَإِذَا تَوَلَّى سَعَىٰ فِي الْأَرْضِ لِيُفْسِدَ فِيهَا وَيُهْلِكَ الْحَرْثَ وَالنَّسْلَ ۗ وَاللَّهُ لَا يُحِبُّ الْفُسَادَ .

Terjemahnya:

Dan apabila ia berpaling (dari kamu), ia berjalan di bumi untuk mengadakan kerusakan padanya, dan merusak tanam-tanaman dan binatang ternak, dan Allah tidak menyukai kebinasaan.⁴

Dari kedua ayat tersebut secara tegas menjelaskan bahwa menjaga ketertiban, keamanan adalah suatu perintah sekaligus adanya ketegasan dari Allah swt. untuk tidak membuat kerusakan baik sesama manusia maupun kepada lingkungan sekitar termasuk binatang dan tanaman.

Dilihat dari sudut pandang hukum pidana Islam yang menjadi landasan pokok terhadap aspek yuridis, adalah teori *maqasid al-syari'ah* meletakkan prinsip-prinsip yang menjadi pertimbangan pokok dari tujuan hukum, yaitu terwujudnya kemaslahatan manusia baik di dunia maupun di akhirat, yaitu terwujud dan terpeliharanya *al-masā'il al-khamsah* atau lima kebutuhan pokok dalam kehidupan manusia yang mencakup pemeliharaan agama (*hifz al-din*), jiwa (*hifz al-nafs*), keturunan atau kehormatan (*hifz al-nasl*), harta (*hifz al-māl*) dan akal (*hifz al-'aql*).⁵

Tindakan pembunuhan dilarang oleh Allah swt. karena dasar pertimbangannya adalah tindakan tersebut dinilai tidak memelihara jiwa (nyawa) seseorang yang dalam agama telah dilindungi sebagai anugrah Allah swt. yang harus

⁴*Ibid.*, h. 32.

⁵Abu Ishak al-Syatibi Ibrahim bin Musa al-Garnati al-Maliki, *al-Muwafaqat fi Ushul al-Syari'ah*, Jilid II (Beirut: Dar al-Kutub al-'Ilmiyyah, [t.th.]), h. 195.

tetap dijaga dan dijunjung tinggi. Demikian juga dengan pencurian, dalam agama harta haruslah dijaga karena menjadi kebutuhan manusia dalam kehidupan sehari-hari.

Dengan pertimbangan tersebut, pencurian dinyatakan dalam Alquran (Q.S. Al-Maidah/5: 38) sebagai berikut:

وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءُ بِمَا كَسَبَا نَكَالًا مِّنَ اللَّهِ وَاللَّهُ عَزِيزٌ حَكِيمٌ

Terjemahnya:

Laki-laki yang mencuri dan perempuan yang mencuri, potonglah tangan keduanya (sebagai) pembalasan bagi apa yang mereka kerjakan dan sebagai siksaan dari Allah. Dan Allah Maha Perkasa lagi Maha Bijaksana.⁶

Pelaku pencurian oleh Allah swt. diberi sanksi dengan potong tangan karena agar pelaku tidak mengulangnya lagi. Hal ini cukup relevan, karena tangan merupakan instrumen yang digunakan oleh pencuri untuk mengambil barang milik orang lain.

Melihat kenyataan tersebut, tindakan-tindakan yang sudah dianggap sebagai tindakan yang menyimpang dari norma hukum yang terjadi di masyarakat menjadi cikal bakal model dan bentuk kejahatan yang terus mengalami perkembangan.

Van Bammelen pernah menyebutkan, bahwa kejahatan adalah setiap perbuatan yang bersifat tidak susila, melanggar norma, mengacaukan, dan menimbulkan banyak ketidaktenangan dalam kehidupan masyarakat, sehingga masyarakat berhak untuk mencela, mereaksi, atau mengatakan penolakannya atas perbuatan itu. Masyarakat berhak untuk membenci segala bentuk tindak kejahatan,

⁶*Ibid.*, h. 32.

karena di dalam kejahatan bukan hanya mengandung perbuatan hukum, tetapi juga melanggar hak-hak sosial, ekonomi, dan lain sebagainya.⁷

Pernyataan Van Bammelen memberikan isyarat bahwa kejahatan yang dilakukan seseorang maupun sekelompok orang dapat mengakibatkan struktur sosial terganggu, karena elemen-elemen yang terbangun di dalam masyarakat berjalan secara tidak sempurna. Hal ini terjadi dalam kurun waktu yang panjang, karena dalam perjalanan sejarah tidak pernah kosong dari kejahatan tersebut.

Apabila ditelusuri lebih jauh kejahatan itu setua usia kehidupan manusia, maka tingkat dan ragam kejahatan juga mengikuti realitas perkembangan kehidupan manusia. Kecenderungan terbukti, bahwa semakin maju dan modern kehidupan masyarakat, maka semakin maju dan modern pula jenis dan modus operandi kejahatan yang terjadi di tengah masyarakat. Hal ini seolah-olah membenarkan suatu adagium, bahwa “di mana ada masyarakat di situ ada kejahatan”.⁸

Faktanya, adagium “di mana ada masyarakat, di situ ada kejahatan” benar terbukti. Realitas perkembangan kehidupan masyarakat di satu sisi memperlihatkan potret yang sebenarnya, bahwa setiap tahapan perkembangan yang terjadi di tengah perubahan sosial bisa diniscayakan diikuti dengan berbagai kenyataan lain yang kurang menyenangkan, sebab realitas yang tidak menyenangkan ini adalah berbentuk perilaku menyimpang.⁹

Fenomena baru yang dapat dirasakan adalah ketika melihat tindakan-tindakan masyarakat yang menyimpang dari norma hukum adalah praktik-praktik di

⁷Achmad Sodiki dalam Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Cet. I; Bandung: Refika Aditama, 2005), h. vii.

⁸*Ibid.*, h. viii.

⁹*Ibid.*

dunia maya (*cyber space*). Di mana para pelaku secara sengaja maupun iseng memasuki area sistem komputer (internet) dengan mengambil sesuatu yang dianggap bernilai baik dalam bentuk dokumen elektronik maupun informasi elektronik ataupun barang berharga yang bukan miliknya secara melawan hukum.

Tindakan tersebut tidak ubahnya seperti yang pernah terjadi seratus tahun bahkan seribu tahun lalu yang dilakukan oleh orang yang memasuki rumah atau pekarangan orang kemudian mengambil sesuatu yang ada di dalamnya tanpa izin yang bertentangan dengan hukum.

Dilihat dari kacamata hukum pidana, kedua hal tersebut sama-sama bertentangan dengan hukum, karena memasuki area yang bukan haknya dan mengambil barang yang bukan miliknya adalah tindakan yang dilarang dan pelakunya patut memperoleh sanksi. Hanya letak perbedaannya pada modus operandi dari perbuatan tersebut.

Demikian halnya dengan hukum pidana Islam, tentu melihat kenyataan itu didasarkan oleh fakta-fakta yang terlihat dari perbuatan dan unsur-unsurnya. Karena dunia *cyber* pada hakikatnya adalah dunia nyata seperti halnya hukum pidana konvensional. Hanya perbedaannya pada modus operandi dari tindakan tersebut. Dalam tinjauan yuridis peristiwa hukum yang dapat diamatai dapat pula dibuktikan.

Karena kejahatan itu mengalami perkembangan, tentu pembuktiannya juga dengan perkembangan yang mengiringi dari kejahatan tersebut. Hal ini cukup beralasan, karena kejahatan selalu berdampingan dengan masyarakat dalam hal ini masyarakat dunia maya.

Oleh karena itu, hukum pidana Islam melihat *cyber crime* sebagai suatu kejahatan nyata yang mengalami modernisasi pada aspek modus operandi dan

memilik kesamaan terhadap hukum pidana Islam pada aspek substansi. Hanya saja pada proses penetapan jenis kejahatan melihat adanya kesamaan unsur-unsur yang melekat pada jenis kejahatan tersebut.

B. Cyber Crime dan Relevansinya dengan Jarimah

Sebelum dijelaskan *cyber crime* dan relevansinya dengan *jarimah*, terlebih dahulu perlu di jelaskan kata *jarimah* dengan jinayah, karena kedua kata tersebut mengandung pengertian yang memiliki kesamaan dan perbedaan. Oleh karena itu, perlu dijelaskan lebih lanjut untuk memperoleh gambaran secara jelas. Di samping itu, kedua kata tersebut seringkali menjebak substansi permasalahan yang ada, sehingga perlu kedua kata tersebut didudukkan pengertiannya secara proporsional.

Rahmat Hakim¹⁰ menjelaskan kesamaan dan perbedaan dari kata *jinayah* dan *jarimah* sebagai dua kata yang memiliki pengertian, arti dan arah yang sama secara etimologis. Selain itu, istilah yang satu menjadi *muradif* (sinonim) bagi istilah lainnya atau keduanya bermakna tunggal. Meskipun demikian, kedua istilah tersebut berbeda dalam penerapannya. Dengan demikian, kedua istilah tersebut harus diperhatikan dan dipahami agar penggunaannya tidak keliru.

Jinayah artinya perbuatan dosa, perbuatan salah atau jahat. *Jinayah* adalah *masdar* (kata asal) dari kata kerja (*fi'il madhi*) *jana* yang mengandung arti suatu kerja yang diperuntukkan bagi satuan laki-laki yang telah berbuat dosa atau salah. Pelaku kejahatan itu sendiri disebut dengan *jani* yang merupakan bentuk *singular* bagi satuan laki-laki atau bentuk *mufrod mudhakara* sebagai pembuat kejahatan atau *isim fa'il*. Adapun sebutan pelaku kejahatan wanita adalah *janiyah*, yang artinya dia

¹⁰Rahmat Hakim, *Hukum Pidana Islam (Fikih Jinayah)* (Cet. I; Bandung: CV Pustaka Setia, 2000), h. 11-15.

(wanita) yang telah berbuat dosa. Orang yang menjadi sasaran atau obyek perbuatan si *jani* atau si *janiyah* atau mereka yang terkena dampak dari perbuatan si pelaku disebut *mujnā'alah* atau korban.¹¹

Abdul Qadir Audah dalam kitab *al-Tasyri' al-Jina'i al-Islamiy* menjelaskan arti kata *jinayah* sebagai berikut:

الْجَنَايَةُ لُغَةً اسْمٌ لِمَا يَجْنِيهِ الْمَرْءُ مِنْ شَرِّ مَا اكْتَسَبَهُ. وَاصْطِلَاحًا اسْمٌ لِفِعْلِ مُحَرَّمٍ شَرْعًا سِوَا مَا وَقَعَ الْفِعْلُ عَلَى نَفْسٍ أَوْ مَالٍ أَوْ غَيْرِ ذَلِكَ.

Artinya:

Jinayah menurut bahasa merupakan nama bagi suatu perbuatan jelek seseorang. Adapun menurut istilah adalah nama bagi suatu perbuatan yang diharamkan syarak, baik perbuatan tersebut mengenai jiwa, harta benda, maupun selain jiwa dan harta benda.¹²

Jadi, pengertian *jinayah* adalah semua perbuatan yang diharamkan. Perbuatan yang diharamkan adalah tindakan yang dilarang atau dicegah oleh syarak (Hukum Islam). Apabila dilakukan perbuatan tersebut mempunyai konsekuensi membahayakan agama, jiwa, akal, kehormatan, dan harta benda.

Menurut Mazhab Hanafi, ada pemisahan dalam pengertian *jinayah* ini. Kata *jinayah* hanya diperuntukkan bagi semua perbuatan yang dilakukan manusia dengan obyek anggota badan dan jiwa, seperti melukai atau membunuh. Adapun perbuatan dosa atau perbuatan salah yang berkaitan dengan obyek atau sasaran barang atau harta benda, dinamakan *gasab*. Oleh karena itu, pembahasan mengenai pencurian dipisahkan dari pembahasan *jinayah*, yang hanya membahas kejahatan atau

¹¹*Ibid.*, h. 12.

¹²Abdul Qadir Audah, *Al-Tasyri' al-Jina'i al-Islamiy*, Juz I (Cet. III; Beirut: Dar Al-Kitab Al'arabi, [t.th]), h. 67.

pelanggaran terhadap jiwa atau anggota badan. Jadi, pembahasan tentang *jinayah* dikhususkan bagi kejahatan terhadap jiwa dan anggota badan, sedangkan masalah yang terkait dengan kejahatan terhadap benda diatur pada bab tersendiri. Adapun mazhab lain seperti Mazhab Syafi'i, Maliki, dan Ibnu Hambal tidak mengadakan pemisahan antara perbuatan jahat terhadap jiwa dan anggota badan dengan kejahatan terhadap harta benda (pencurian dan kejahatan terhadap harta benda lainnya). Oleh karena itu, pembahasan keduanya (kejahatan terhadap anggota badan, jiwa dan harta benda) diperoleh dalam *jinayah*.¹³

Berdasarkan hal tersebut, kata *jinayah* yang berarti perbuatan jahat, salah, atau pelanggaran sudah inklusif (mencakup) segala bentuk kejahatan, baik terhadap jiwa ataupun anggota badan. Kejahatan terhadap harta benda secara otomatis termasuk dalam pembahasan *jinayah* tanpa perlu diadakan pemisahan dalam pembahasan di antara keduanya.

Di samping itu, pengertian *jinayah* pada awalnya diartikan hanya bagi semua jenis perbuatan yang dilarang. Jadi, melalaikan perbuatan yang diperintahkan dalam konteks pengertian tersebut bukanlah *jinayah*. Padahal semua perbuatan dosa, perbuatan salah, dan sejenisnya dapat berupa perbuatan ataupun berupa meninggalkan perbuatan yang diperintahkan melakukannya. Hal ini karena pelanggaran terhadap peraturan dapat berbentuk mengerjakan suatu perbuatan yang dilarang (bersifat aktif) atau meninggalkan perbuatan yang berdasarkan hukum harus dikerjakan (bersifat pasif).

Sedangkan kata *jarimah* mengandung arti perbuatan buruk, jelek, atau dosa. Jadi pengertian *jarimah* secara harfiah sama halnya dengan pengertiannya *jinayah*.

¹³Rahmat Hakim, *op. cit.*, h. 13.

Adapun pengertian *jarimah* sebagaimana dikemukakan oleh Imam al-Mawardi adalah sebagai berikut:

الْجَرَائِمُ مَحْظُورَاتٌ شَرْعِيَّةٌ زَجَرَاللَّهُ تَعَالَى عَنْهَا بِحَدِّ أَوْ تَعْزِيرٍ.

Artinya:

Jarimah adalah perbuatan-perbuatan yang dilarangan oleh syarak yang dincam oleh Allah dengan hukuman had atau takzir.¹⁴

Dalam hal ini, sebagaimana halnya kata *jinayah* kata *jarimah* pun mencakup perbuatan ataupun tidak berbuat, mengerjakan atau meninggalkan, aktif atau pasif. Oleh karena itu, perbuatan *jarimah* tidak saja mengerjakan perbuatan yang jelas-jelas dilarang oleh peraturan, tetapi juga dianggap sebagai *jarimah* kalau seseorang meninggalkan perbuatan yang menurut peraturan harus dia kerjakan. Abdul Qadir Audah menjelaskan masalah ini dengan mengatakan bahwa kata larangan (مَحْظُورَاتٌ) seperti yang termaktub dalam definisi di atas menjelaskan sebagai berikut:

أَمَّا تَيَانُ فِعْلٍ مَنَّهُ عَنهُ أَوْ تَرَكَ فِعْلٍ مَأْمُورٍ بِهِ.

Artinya:

Yang dimaksud dengan *mahdhurat* (larangan) adalah melakukan suatu perbuatan yang dilarang atau meninggalkan suatu perbuatan yang diperintahkan.¹⁵

Dari penjelasan tersebut dapat dipahami bahwa kata *mahdhurat* mengandung dua pengertian. *Pertama*, larangan berbuat artinya dilarang mengerjakan perbuatan

¹⁴Abu al-Hasan al-Mawardi, *Al-Ahkam al-Sultaniyyah* (Cet. II; Mesir: Mustafa al-Babi al-Halabi, 1975), h. 219.

¹⁵Rahmat Hakim, *op. cit.*, h. 14.

yang dilarang. *Kedua*, larangan tidak berbuat atau larangan untuk diam artinya meninggalkan (diam) terhadap perbuatan yang menurut peraturan harus dia kerjakan. Meskipun pengertian *jinayah* dengan *jarimah* sulit dipisahkan dalam pemakaian sehari-hari, kedua kata tersebut dapat dibedakan.

Kata jarimah, sering digunakan sebagai perbuatan dosa bentuk, macam, atau sifat dari perbuatan dosa besar tersebut. Misalnya, pencurian, pembunuhan, perkosaan, atau perbuatan yang berkaitan dengan politik. Keseluruhan itu dapat disebut dengan istilah jarimah yang kemudian dirangkaikan dengan satuan atau sifat perbuatan tersebut. Oleh karena itu, menggunakan istilah *jarimah* pencurian, *jarimah* pembunuhan, *jarimah* perkosaan, dan *jarimah* politik dan tidak menggunakan istilah *jinayah* pencurian, *jinayah* pembunuhan, *jinayah* perkosaan, dan *jinayah* politik.

Dari uraian tersebut, dapat diambil pengertian bahwa kata *jarimah* identik dengan pengertian yang disebut dalam hukum positif sebagai tindak pidana atau pelanggaran. Hal tersebut maksudnya adalah satuan atau sifat dari suatu pelanggaran hukum. Dalam hukum positif, contoh-contoh *jarimah* di atas diistilahkan dengan tindak pidana pencurian, tindak pidana pembunuhan.

Jadi, dalam hukum positif *jarimah* diistilahkan dengan delik atau tindak pidana. Dalam hukum positif juga dikenal istilah perbuatan pidana, peristiwa pidana, pelanggaran pidana, perbuatan yang boleh dihukum yang artinya sama dengan delik. Keseluruhan itu merupakan pengalihan dari Bahasa Belanda, *strafbaar fait*. Dalam pemakaian istilah delik lebih sering digunakan dalam ilmu hukum secara umum, sedangkan istilah tindak pidana seringkali dikaitkan terhadap korupsi yang dalam undang-undang sering digunakan istilah perbuatan pidana.

Dengan demikian dapatlah disimpulkan, bahwa dari kedua istilah tersebut memiliki kesamaan dan perbedaan secara etimologis. Kedua istilah tersebut bermakna tunggal, memiliki arti yang tunggal dan memiliki arti yang sama serta ditujukan bagi perbuatan yang berkonotasi negatif, salah dan dosa. Adapun perbedaannya terletak pada pemakaian, arah pembicaraan, serta dalam rangkaian apa kedua kata tersebut digunakan.

Penjelasan tersebut memberikan gambaran secara jelas, bahwa *jarimah* sebagaimana yang dimaksud dalam hukum pidana Islam adalah delik atau tindak pidana. Hal ini apabila dikaitkan dengan tindak pidana *cyber crime*, maka *cyber crime* menjadi bagian dari obyek yang sama dari *jarimah*, hanya *cyber crime* merupakan tindak pidana yang dilakukan melalui media elektronik dan sejenisnya, sementara *jarimah* dilakukan dalam dunia *real* (dunia nyata) sebagaimana dalam hukum konvensional.

Melihat kenyataan dalam dunia *cyber*, hukum ruang maya haruslah juga difokuskan dalam pembahasan hukum pidana Islam, karena undang-undang yang ada belumlah maksimal dalam penerapannya. Hal ini terjadi karena undang-undang yang ada sebagai produk hukum tidak di gali dari sumber yang jernih. Berbeda halnya dengan hukum pidana Islam yang jelas sumber hukumnya memiliki kejernihan, yakni sumber hukum dari Allah. Kejernihan dan kemurnian sumber inilah yang dapat melahirkan sebuah produk hukum yang dapat dipertanggungjawabkan dari pada produk hukum yang bersumber dari Hukum Eropa Kontinental.

Secara filosofis dapat digambarkan, bahwa sesuatu yang jernih itu lahir dari yang jernih, sementara sesuatu yang tidak jernih itu sulit melahirkan sebuah kejernihan dan bahkan tidak dapat menghasilkan kejernihan. Hal ini secara tersirat

menggambarkan, bahwa produk hukum haruslah dibuat oleh orang-orang yang memiliki kredibilitas dan niat yang benar untuk bisa menghasilkan undang-undang yang benar pula sehingga dapat mencapai sebuah tujuan hukum, yakni terciptanya rasa keadilan, kesejahteraan, ketentraman dan kedamaian masyarakat.

Berkaitan dengan hal tersebut, *cyber crime* tentu memiliki relevansi dengan *jarimah* karena dalam sebuah negara yang menerapkan hukum Islam tentu *cyber crime* menjadi obyek dari *jarimah* itu sendiri. Rumusan dalam *cyber crime* tidak jauh berbeda dengan *jarimah* yang membedakan di antara keduanya terletak pada modus operandinya. Selain itu, hukum pidana juga dapat menggali melalui teknik dan cara yang sudah dirumuskan oleh para ulama fikih, khususnya fikih *jinayah*.

Suatu perbuatan dinamakan *jarimah* (tindak pidana, peristiwa pidana atau delik) apabila perbuatan tersebut mengakibatkan kerugian bagi orang lain atau masyarakat baik jasad (anggota badan atau jiwa), harta benda, keamanan, tata aturan masyarakat, nama baik, perasaan ataupun hal-hal lain yang harus dipelihara dan dijunjung tinggi keberadaannya. *Cyber crime* sampai hari ini terjadi dalam jumlah yang sulit untuk dihitung, karena lajunya lalu lintas di dunia *cyber* berdampak terhadap perilaku dari pengguna layanan internet. Hal ini tentu mengakibatkan jumlah kerugian terhadap harta benda dan kemanan yang sangat besar.

Media elektronik dan *on line* menjadi alternatif dalam melakukan transaksi bisnis, seperti (*e-commerce*). Kegiatan perdagangan yang dilakukan melalui layanan elektronik, dalam hal ini melalui sarana internet, baik sistem promosi, sistem transaksi, sistem pembayarannya memiliki konsekuensi yang sangat rentan terhadap tindak kejahatan. Hal ini jika tidak berhati-hati dapat terjadi kecurangan yang pelaku dari bisnis tersebut tidak dapat diketahui, karena karakter dari bisnis ini tidak

berhadapan langsung dengan pihak ke dua. Oleh karena itu, perbuatan pidana sangat berpeluang dilakukan melalui media elektronik ini. Hal ini, tentu perbuatan dari orang-orang yang tidak bertanggung jawab sangat merugikan pihak-pihak yang bertransaksi.

Jadi, yang menyebabkan suatu perbuatan tersebut dianggap sebagai suatu *jarimah* adalah dampak dari perilaku tersebut yang menyebabkan kerugian kepada pihak lain, baik dalam bentuk material (jasad, nyawa atau harta benda) maupun nonmateri atau gangguan nonfisik, seperti ketenangan, ketentraman, harga diri, adat istiadat, dan sebagainya.

Penyebab perbuatan yang merugikan tersebut di antaranya adalah tabiat manusia yang cenderung pada sesuatu yang menguntungkan bagi dirinya meskipun hasil pilihan atau perbuatan tersebut merugikan orang lain. Kenyataan ini memerlukan kehadiran peraturan atau undang-undang. Akan tetapi, kehadiran peraturan tersebut menjadi tidak berarti tanpa adanya dukungan yang dapat memaksa seseorang untuk mematuhi peraturan tersebut. Dukungan yang dimaksud adalah penyertaan ancaman hukuman atau sanksi yang menyertai kehadiran peraturan tersebut.

Dengan demikian, tindak pidana dalam dunia *cyber* menjadi bagian dari obyek yang sama dari perbuatan-perbuatan pidana yang dapat dikategorikan sebagaimana *jarimah* dalam hukum pidana Islam. Yang perlu ditegaskan dalam hal ini adalah sejauhmana penyelesaian perbuatan pidana dalam dunia *cyber* menurut rumusan-rumusan yang ditetapkan dalam hukum pidana Islam. Apakah hukum pidana Islam memiliki rumusan yang sama dalam hal karakteristik dari tindak pidana dalam ruang *cyber*? Hal ini membutuhkan kajian yang mendalam terhadap *cyber*

crime untuk dapat memperoleh gambaran yang utuh sebagai parameter dalam merumuskan tindak pidana tersebut ke dalam suatu rumusan sebagaimana hukum pidana Islam.

C. Cyber Crime dan Korelasinya dalam Pembagian Hukum Pidana Islam

Ditinjau dari aspek hukumnya, *jarimah* apabila dilihat menurut hukum pidana Islam terbagi atas 3 (tiga) macam bentuk, yaitu *jarimah hadd*, *jarimah qisas* dan *diat*, dan *jarimah takzir*.

1. Jarimah Hadd

Jarimah hadd adalah *jarimah* yang diancam dengan hukuman *hdd*. Pengertian hukuman *hdd* sebagaimana dikemukakan oleh Abdul Qadir Audah adalah:

وَالْحَدُّ هُوَ الْعُقُوبَةُ الْمَقْدَرَةُ حَقَّالِلَّهِ تَعَالَى.

Artinya:

Hukuman *hdd* adalah hukuman yang telah ditentukan oleh syarak dan merupakan hak Allah.¹⁶

Dari pengertian tersebut dapat diketahui bahwa ciri khas *jarimah hadd* itu sebagai berikut:

- a. Hukumannya tertentu dan terbatas, dalam arti bahwa hukuman tersebut telah ditentukan oleh syarak dan tidak ada batas minimal dan maksimal.
- b. Hukuman tersebut merupakan hak Allah semata-mata, atau kalau ada hak manusia di samping hak Allah, maka hak Allah yang lebih dominan.

¹⁶Abd. Qadir Audah, I, *op. cit.* h. 79.

Oleh karena hukuman *hdd* itu merupakan hak Allah, maka hukuman tersebut tidak bisa digugurkan oleh perseorangan (orang yang menjadi korban atau keluarganya) atau oleh masyarakat yang diwakili oleh negara.

Jarimah hdd ini ada beberapa macam, yaitu:

- 1) *Jarimah zina*,
- 2) *Jarimah qadaf*,
- 3) *Jarimah syurb al-khamr* dan perjudian (undian),
- 4) *Jarimah* pencurian dan penipuan,
- 5) *Jarimah hirabah* (penodongan atau perampokan),
- 6) *Jarimah riddah*, dan
- 7) *Jarimah* pemberontakan/*subversive* (*al-bagyu*).

2. *Jarimah Qisds* dan Diat

Jarimah qisds dan diat adalah *jarimah* yang diancamkan dengan hukuman *qisds* atau diat. *Jarimah qisds* maupun diat kedua-duanya adalah hukuman yang sudah ditentukan oleh syarak. Perbedaannya dengan hukuman *hdd* adalah bahwa hukuman *hdd* merupakan hak Allah (hak masyarakat), sedangkan *qisds* dan diat merupakan hak manusia (hak individu). Di samping itu, perbedaan yang lain adalah karena hukuman *qisds* dan diat merupakan hak manusia, maka hukuman tersebut bisa dimaafkan atau digugurkan oleh korban atau keluarganya, sedangkan hukuman *had* tidak bisa dimaafkan atau digugurkan.

Pengertian *qisds* sebagaimana dikemukakan oleh Muhammad Abu Zahrah adalah:

المساواة بين الجريمة والعقوبة

Artinya:

Persamaan dan keseimbangan antara *jarimah* dan hukuman.¹⁷

Jarimah qisas dan diat ini hanya ada 2 (dua) macam, yaitu pembunuhan dan penganiayaan. Namun apabila diperluas, jumlahnya ada lima macam, yaitu:

- a. Pembunuhan sengaja (الْقَتْلُ الْعَمْدُ)
- b. Pembunuhan menyerupai sengaja (الْقَتْلُ شَبْهُ الْعَمْدِ)
- c. Pembunuhan karena kesalahan (الْقَتْلُ الْخَطَأُ)
- d. Penganiayaan sengaja (الْجَنَایَةُ عَلَى مَا دُونَ النَّفْسِ عَمْدًا)
- e. Penganiayaan tidak sengaja (الْجَنَایَةُ عَلَى مَا دُونَ النَّفْسِ خَطَأً).¹⁸

3. *Jarimah* Takzir

Jarimah takzir adalah *jarimah* yang diancam dengan hukuman takzir. Pengertian takzir menurut bahasa adalah *ta'dib*, artinya pemberi pelajaran.¹⁹ Takzir diartikan dengan *al-Raddu wal Man'u*, yang artinya menolak dan mencegah.²⁰ Sedangkan pengertian takzir menurut istilah, sebagaimana dikemukakan oleh Al-Mawardi adalah:

وَالْتَعْزِيرُ تَأْدِيبٌ عَلَى ذُنُوبٍ لَمْ تُشْرَعْ فِيهَا الْحُدُودُ.

UNIVERSITAS ALAUDDIN
MAKASSAR

¹⁷Muhammad Abu Zahrah, *Al-Jarimah wa al-'Uqubah fi al-Fikr al-Islamiy* ([t.t.]: Dar al-Fikr al-'Arabi, [t.th]), h. 380.

¹⁸Abd. Qadir Audah, *loc. cit.*

¹⁹Abd. Qadir Audah, *op. cit.*, h. 80.

²⁰Abd. Aziz 'Amir, *Al-Ta'zir fi al-Syari'ah al-Islamiyah* (Cet. IV; [t.t]: Dar al-Fikr al-'Arabi, 1969), h. 52.

Artinya:

Takzir adalah hukuman pendidikan atas dosa (tindak pidana) yang belum ditentukan hukumannya oleh syarak.²¹

Dari definisi tersebut dapat diketahui bahwa hukuman takzir adalah hukuman yang belum ditetapkan syarak, dan wewenang untuk menetapkan diserahkan kepada ulil amri. Di samping itu, dari definisi tersebut dapat diketahui bahwa ciri khas *jarimah* takzir adalah sebagai berikut:

- a. Hukumannya tidak tetentu dan tidak terbatas. Artinya hukuman tersebut belum ditentukan oleh syarak dan batas minimal dan maksimal.
- b. Penentuan hukuman tersebut adalah hak penguasa (ulil amri).

Berdasarkan uraian dari pembagian *jarimah* dalam hukum pidana Islam tersebut, maka *cyber crime* tergolong dalam *jarimah* takzir. Hal ini di dasarkan atas ketiadaan teks Alquran yang menjelaskan terhadap persoalan *cyber crime*. Akan tetapi apabila ditelusuri lebih jauh, maka dapat ditemukan *jarimah* dalam kategori *jarimah h~~u~~duh*, di antaranya adalah tuduhan berbuat zina (pencemaran nama baik), perjudian atau undian, pencurian, dan penipuan.

Sedangkan pada kasus-kasus yang lainnya yang disebutkan dalam *jarimah h~~u~~duh* tidak masuk dalam pembahasannya, karena kasus-kasus tersebut lebih terfokus pada adanya perbuatan pidana yang harus melibatkan kontak fisik secara langsung. Sedangkan bentuk *jarimah* yang lainnya terjadi tanpa melibatkan kontak fisik. Secara umum *cyber crime* lebih menitik beratkan jenis kasus-kasus pidana yang tidak secara langsung terjadinya kontak fisik, sehingga kasus-kasus yang

²¹Al-Mawardi, *op. cit.*, h. 236.

melibatkan kontak fisik tidak terakomodir. Misalnya, jarimah zina, pemberontakan, meminum khamar, penodongan dan perampokan, pemberontakan, dan *riddah* (murtad).

Misalnya dalam Pasal 30 ayat (1), (2), dan (3) dalam Undang-Undang ITE menjadi dasar hukum terhadap kasus kejahatan *carding* (kejahatan kartu kredit). Terhadap kasus ini ada beberapa kemungkinan yang dapat dilakukan oleh pelaku kejahatan *carding*, yaitu pencurian atau penggelapan.

Pelaku dapat dikatakan pencurian karena mengambil barang yang bukan haknya dengan cara yang tidak sah. Obyek pencurian dapat bermacam-macam. Sering kali data komputer lebih menarik, karena berisi rahasia yang sangat bernilai untuk dijual. Sering juga manipulasi itu digunakan untuk memperoleh keuntungan keuangan atau barang.

Salah satu contoh kasus yang lazim dilakukan ialah, petugas komputer perusahaan mencari sejumlah barang dengan mengubah data komputer yang berisi daftar barang. Dengan perubahan data tersebut, dimaksudkan untuk menghilangkan sejumlah barang sehingga pelaku dapat memiliki barang tanpa terlihat dalam laporan bulanan. Biasanya sesudah berlangsung lama kehilangan baru dapat diketahui.²² Contoh yang lain misalnya, dengan modus *electronic piggyhacking*,²³ pencurian *software*,²⁴ penyalahgunaan *cash-card*.²⁵

²²Ninie Suparni, *Cyber Space: Problematika dan Antisipasi Pengaturannya* (Cet. I; Jakarta: Sinar Grafika, 2009), h. 155.

²³*Electronic Piggyhacking* ialah modus pencurian dengan menyembunyikan terminal atau alat penghubung ke dalam sistem komputer secara diam-diam. Dengan melalui terminal tersebut, data komputer dapat dipelajari atau ditransfer untuk dicuri apabila komputer sedang tidak dipergunakan.

²⁴Pencurian *Software* ialah mengambil data komputer secara tidak sah atau menggelapkan tanpa mengambil disket (*hard disk*) atau *carrier* yang berisi data. Dengan memasuki sistem komputer secara melawan hukum, pelaku mentransfer data ke dalam komputernya di tempat lain atau membuat *copy* data komputer tertentu.

Disebut penggelapan, karena menggunakan cara yang lazim digunakan dengan memasukkan keterangan palsu ke dalam data komputer, yang dapat dilakukan dengan mengubah data atau menambah data tersebut. Perbuatan tersebut dikenal dengan nama data *diddling*. Pemrosesan data dari suatu perusahaan besar seperti bank, biasanya melibatkan beberapa orang, seperti yang membuat program, yang mencatat atau memasukkan data, yang mengirimkan, yang memberikan kode, yang melakukan pengecekan dan lainnya.²⁶

Kemungkinan pemalsuan data dapat dilakukan dalam salah satu proses tersebut, terlebih jika ada kerja sama antara semua petugas komputer, proses memanipulasi data dapat berjalan dengan lancar. Manipulasi data dapat dilakukan, misalnya dengan memalsukan dokumen yang akan dimasukkan, mengganti disket dengan yang palsu yang telah dipersiapkan sebelumnya, atau mengubah sumber data.

Hal tersebut dapat dilihat pada kasus pembobolan kartu kredit melalui internet dengan tersangka Petrus Pangkur alias Bony Diobok-obok, yang diputus oleh Pengadilan Negeri Sleman dengan hukuman satu tahun penjara.²⁷

Berdasarkan contoh kasus di atas, maka apabila pencurian dilakukan dengan melebihi batas minimal (yakni, mencapai satu nishab²⁸) sebagaimana dalam *jarimah*

²⁵Penyalahgunaan *Cash-Card* adalah mengambil uang dari mesin otomatis seperti *cash dispenser* atau *automatic teller machine (ATM)* melebihi dana yang ada atau dananya sudah tidak ada, di mana penyerahan uang oleh ATM tanpa menipu atau memanipulasi data komputer, yaitu dengan menggunakan *password* atau PIN yang sah.

²⁶Niniek Suparni, *op. cit.*, h. 154.

²⁷Sutarman, *Cyber Crime: Modus Operandi dan Penanggulangannya* (Cet. I; Yogyakarta: Laksbang Pressindo, 2007), h. 65.

²⁸Tindak pidana pencurian dapat dikenakan hukuman apabila barang yang dicuri telah mencapai satu nisab. Hal ini ditegaskan dalam hadis Nabi saw. yang diriwayatkan oleh Imam al-Bukhari sebagai berikut:

تُقَطَّعُ الْيَدَيْنِ رُبْعَ دِينَارٍ فَصَاعِدًا

pencurian, maka dapat digolongkan sebagai *jarimah hudud*. Demikian halnya apabila pencurian dilakukan tidak mencapai batas satu nisabnya, maka pencurian tersebut digolongkan dalam *jarimah takzir*.

Sedangkan penipuan adalah mengambil hak orang lain secara licik atau curang sehingga orang lain mengalami kerugian.²⁹ Apabila ditinjau dari tujuan hukum, akibat penipuan pihak tertipu dirugikan. Perbedaannya dengan tindak pidana pencurian, yaitu kesalahan bukan hanya pada pihak penipu, melainkan pihak pemilik harta juga bersalah, yaitu karena kebodohnya, sehingga ia tertipu.

Berdasarkan hal tersebut di atas, penipuan dalam *cyber crime* jauh lebih rentan terjadi dibandingkan dengan penipuan secara tradisional. Hal ini terjadi karena sifat dari dunia *cyber* adalah karena obyeknya tidak terlihat jelas secara kasat mata, melainkan berada di balik program komputer.

Penipuan komputer (*computer fraud*) dapat terjadi atas beberapa jenis:³⁰

1. Bentuk dan jenis penipuan, yaitu berupa pencurian uang atau harta benda menggunakan sarana komputer dengan melawan hukum, yaitu dalam bentuk penipuan data dan penipuan program sebagai berikut:
 - a. Memasukkan instruksi tidak sah, dilakukan orang yang berwenang atau tidak, yang dapat mengakses suatu sistem, memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (misalnya transfer).

Artinya:

Tangan pencuri dipotong dalam pencurian seperempat dinar ke atas.

²⁹Zainuddin Ali, *op. cit.*, h. 118.

³⁰Ninie Suparni, *op. cit.*, h. 142-143.

- b. Mengubah data *input*, dilakukan seseorang dengan cara memasukkan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum (misalnya memasukkan data gaji pegawai melebihi seharusnya).
 - c. Merusak data, dilakukan seseorang untuk merusak *print-out* atau *output* dengan maksud mengaburkan, menyembunyikan data atau informasi dengan iktikad tidak baik.
 - d. Penggunaan komputer untuk sarana melakukan perbuatan pidana, yaitu dalam pemecahan informasi melalui komputer yang aslinya digunakan untuk melakukan kejahatan, atau mengubah program.
2. Perbuatan pidana penipuan pada dasarnya termasuk unsur perbuatan lain, dimaksudkan menghindarkan diri dari kewajiban (misalnya pajak) atau memperoleh sesuatu yang bukan hak atau miliknya melalui sarana komputer.
 3. Perbuatan curang memperoleh secara tidak sah harta benda milik orang lain, misalnya seseorang yang dapat mengakses komputer mentransfer rekening orang ke rekeningnya sendiri, sehingga merugikan orang lain.
 4. Konspirasi penipuan adalah perbuatan pidana yang dilakukan beberapa orang bersama-sama untuk melakukan penipuan dengan sarana komputer.
 5. Penipuan yang dilakukan terhadap perusahaan yang berkecimpung dalam kegiatan keuangan, seperti bank, asuransi dan perusahaan besar lainnya yang banyak menggunakan komputer. Para pelakunya selain perorangan (*occupational crime*) juga persahaan itu sendiri (*corporate crime*) yang dengan memanipulasi data keuangan diharapkan untuk memperoleh keuntungan keuangan, misalnya untuk menghindari pembayaran pajak dan lainnya. Cara melakukan penipuan, yaitu dengan memanipulasi atau mengubah data komputer dengan informasi palsu

agar memperoleh keuntungan, baik bagi pelaku maupun perusahaan itu sendiri maupun orang lain.

Kejahatan tersebut dapat terjadi dengan sangat mudah sepanjang pelaku kejahatan memiliki kemampuan dalam mengoperasikan komputer dengan baik. Oleh karena itu, Pasal 28 ayat (1) Undang-Undang ITE dengan tegas mengkriminalkan pelaku penipuan dalam bentuk apapun melalui media *on line* (komputer). Hal ini, tentu terlihat dengan jelas penipuan masuk dalam *jarimah hudud*, sebagaimana uraian dalam pembagian hukum pidana Islam.

Hal serupa dapat dilihat dalam jarimah perjudian. Perjudian dimasukkan dalam jarimah hudud, karena perbuatan pidana ini telah diatur dalam syarak.

Perjudian yaitu mengambil keuntungan dari bentuk permainan, seperti domino atau joker, adu ayam, main bola, dan lain-lain permainan yang tidak memicu pelakunya berbuat kreatif.³¹

Perjudian dimasukkan dalam kelompok *jarimah hudud*, karena jika dilihat dari aspek hukum Islam larangan tentang perjudian dan undian dirangkaikan dengan khamar. Atas dasar tersebut cukup beralasan apabila perjudian dan undian termasuk salah satu obyek kajian pidana Islam, yang konsekuensinya atau sanksi hukumnya disejajarkan dengan tindak pidana khamar.

Hal tersebut, dapat dikorelasikan dengan tindak pidana perjudian (undian) sebagaimana dalam *cyber crime* pada Pasal 27 ayat (2) Undang-Undang ITE. Mencermati klausul rumusan dalam pasal tersebut, bahwa pelaku kejahatan yang dinilai tindak pidana hanyalah orang yang mendistribusikan, mentransmisikan, atau

³¹Zainuddin Ali, *op. cit.*, h. 115.

membuat media perjudian dalam bentuk informasi elektronik atau dokumen elektronik yang bermuatan perjudian.

Klausul pada pasal tersebut sepintas tidak mengaitkan pengguna (*user*) sebagai sasaran yang harus dipidana sebagaimana sasaran hukum pidana Islam. Akan tetapi, hukum pidana Islam tidak melihat apakah pelaku sebagai pengguna ataupun penyedia layanan perjudian, melainkan mengkriminalkan kedua-duanya dan digolongkan sebagai perjudian. Hal ini di dasarkan oleh ayat Alquran, Q.S. al-Maidah/5: 90 sebagai berikut:

يَا أَيُّهَا الَّذِينَ آمَنُوا إِنَّمَا الْخَمْرُ وَالْمَيْسِرُ وَالْأَنْصَابُ وَالْأَزْلَامُ رِجْسٌ مِّنْ عَمَلِ الشَّيْطَانِ فَاجْتَنِبُوهُ لَعَلَّكُمْ تُفْلِحُونَ

Terjemahnya:

Wahai orang-orang yang beriman, sesungguhnya (meminum) khamar, berjudi (berkurban untuk) berhala, mengundi nasib dengan panah, adalah perbuatan keji termasuk perbuatan setan. Maka jauhilah perbuatan-perbuatan itu agar kamu mendapat keberuntungan.³²

Ayat tersebut di atas, memberikan ketegasan bahwa perjudian dan mengundi nasib melalui undian adalah perbuatan keji dan biadab. Larangan perjudian dan mengundi nasib tidak hanya sekedar pelaku terhadap perjudian dan mengundi nasib, akan tetapi juga produsen atau penyedia alat-alat perjudian.

Berdasarkan ayat tersebut, perjudian dikelompokkan dalam *jarimah hudud* yang sanksinya telah ditetapkan oleh syarak.

Untuk pembagian *jarimah qisas* dan diat jenis tindak pidana sebagaimana yang disebutkan di atas, *cyber crime* tidak terakomodir karena dalam *jarimah* ini

³²Departemen Agama RI., *op. cit.*, h. 123.

secara penuh membutuhkan hadirnya person-person dalam perbuatan pidana. Artinya secara fisik keduanya harus hadir sehingga perbuatan pidana dapat terjadi. Misalnya pembunuhan, tentu perbuatan pembunuhan tidak akan terjadi di ruang *cyber*. Demikian halnya tindak pidana penganiayaan juga tidak akan terjadi di dunia *cyber*. Sehingga jenis kejahatan yang termasuk *jarimah qisq* dan diat tidak akan mungkin terjadi di ruang maya (*cyber space*).

Sedangkan dalam kelompok *jarimah takzir* banyak ditemukan pada kejahatan *cyber crime*, karena dasar tindak pidana ini tidak ditemukan dalam Alquran atau hukum syarak yang tidak ditetapkan oleh Allah SWT (*syari'*). Hal ini dapat dilihat pada Pasal 27 ayat (1) tentang Pornografi, Pasal 29 tentang Pengancaman, Pasal 33 tentang Sabotase dan Pengrusakan Undang-Undang ITE dan lain-lain.

Terkait dengan Pasal 27 ayat (1) Undang-Undang ITE tentang Pornografi banyak ditemukan dalam kasus penyebaran foto atau film pribadi seseorang yang vulgar di internet, misalnya kasus Sukma Ayu-Bjah, Ariel-Luna Maya atau Ariel-Cut Tari. Contoh lain misalnya, pada bulan Mei 2003 Satuan Reskrimsus *cyber crime* Polda Metro Jaya menangkap mucikari *cyber*. Pelakunya sepasang suami istri, Ramdoni alias Rino dan Yanti Sari alias Bela. Prostitusi *cyber* ini adalah modus baru yang menawarkan berbagai wanita melalui sebuah alamat *web*.³³

Dalam *web* tersebut ditampilkan deretan foto wanita dalam bentuk *close up* atau dalam busana minim, yang siap melayani pria. Pengelola situs terlihat tidak memiliki rasa malu dengan menampilkan nomor telepon genggamnya, sehingga para

³³Sutarman, *op. cit.*, h. 67.

peminat dapat memesan wanita-wanita yang dikehendaki, kemudian pesanan tersebut di antar ke hotel atau apartemen sesuai pesanan.³⁴

Demikian juga pada Pasal 29 tentang Pengancaman, dimana pelaku seringkali mengirim pesan singkat melalui (SMS) kepada seseorang untuk memperoleh keuntungan melalui ancaman tersebut. Dalam kasus ini juga sering terdengar dan terlihat di media elektronik dan media massa adanya ancaman melalui SMS tentang ancaman bom. Terhadap kasus ini tentu masyarakat menjadi terancam dan merasa keamanannya terganggu bahkan sangat meresahkan.

Sedangkan pada Pasal 30 tentang Pengrusakan dalam Undang-Undang ITE dapat ditemukan kasusnya dalam kejahatan computer sebagai berikut:³⁵

1. *To frustrate data communication* yaitu suatu perbuatan yang dilakukan dengan suatu kesengajaan untuk merusak atau menghancurkan media disket dan media penyimpan sejenis lainnya yang berisikan data atau program yang dimaksud menjadi tidak berfungsi, dan pekerjaan-pekerjaan yang melalui proses computer tidak dapat dilaksanakan.
2. Penghambatan, yaitu dengan sengaja memasukkan, mengubah, menghapuskan atau menempatkan di luar fungsi data komputer atau program komputer dengan maksud untuk menghambat berfungsinya sistem komputer atau sistem telekomunikasi.
3. Perbuatan pidana perusakan sistem komputer, baik merusak data atau menghapus kode sehingga menimbulkan kerusakan dan kerugian. Termasuk, penambahan atau perubahan program, informasi, media, sehingga merusak sistem, juga

³⁴ *Ibid.*

³⁵ Niniek Suparni, *op. cit.*, h. 175-176.

menyebarkan virus yang dapat merusak program dan sistem komputer, atau pemerasan dengan menggunakan sarana komputer maupun telekomunikasi. Contoh kasus pengrusakan melalui penyebaran virus "*I Love You*" atau "*Love Bug*" beserta variasinya yang menyebar dengan cepat diketahui berasal dari Philipina. Virus-virus tersebut sejauh ini menimbulkan kerusakan sangat besar dalam sejarah yang diyakini merupakan manifestasi dari *cyber-terrorism*. Berdasarkan perkiraan virus "*I Love You*" dapat merasuki computer dan jaringan dunia yang menimbulkan kerugian finansial yang besar pada jaringan computer di Malaysia, Jerman, Belgia, Perancis, Swedia, Hongkong, Inggris Raya, dan Amerika Serikat.³⁶ Virus ini menyebabkan ATM-ATM di Belgia tidak berfungsi beberapa waktu dan mengganggu sistem komunikasi internal Majelis Perwakilan Rendah (*The House of Common*) di Inggris, dan menghilangkan sistem surat elektronik (*e-mail*) pada kongres Amerika Serikat.³⁷

4. *The Trojan Horse*, yaitu memanipulasi data atau program dengan jalan mengubah data atau instruksi data pada sebuah program, menghapus, menambah, menjadi—kan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain.

Kasus-kasus seperti tersebut di atas, sering ditemukan dalam ruang *cyber*, karena para hacker menyenangi dan memiliki hobi memasuki situs terlarang yang bukan haknya untuk dapat memperoleh data atau dapat juga hanya sekedar iseng-iseng belaka.

Dalam kasus-kasus di atas, jika dihubungkan dalam hukum pidana Islam masuk dalam *jarimah* takzir, karena sanksi hukumnya tidak ditetapkan dalam syarak.

³⁶Sutarman, *op. cit.*, h. 70-71.

³⁷*Ibid.*, h. 71.

D. Pembuktian Cyber Crime dalam Hukum Pidana Islam

Sebagaimana telah dijelaskan pada pembahasan sebelumnya, bahwa pembuktian pada dasarnya ingin mencari kebenaran materiil. Untuk itu, sistem pembuktian sebagaimana sistem pembuktian dalam hukum konvensional, alat bukti haruslah di dasarkan oleh undang-undang (hukum) yang berlaku. Alat bukti yang berlaku di dalam hukum Islam, tentu sudah diatur dalam Alquran yang termanifestasi dalam sistem hukum pidana Islam.

Berkaitan dengan alat bukti, para ulama berbeda pendapat mengenai jenis-jenis alat bukti tersebut. Perbedaan tersebut dapat dikelompokkan menjadi dua kelompok sebagai berikut:³⁸

Pertama, menurut jumhur ulama, untuk pembuktian *jarimah qisas* dan diat dapat digunakan tiga cara (alat) pembuktian, yaitu:

1. Pengakuan (الإقرار);
2. Persaksian (الشهادة);
3. Al-qasamah (القسم);

Kedua, menurut sebagian fukaha seperti Ibnu al-Qayyim dari mazhab Hambali, untuk pembuktian *jarimah qisas* dan diat digunakan empat cara (alat) pembuktian:

1. Pengakuan (الإقرار);
2. Persaksian (الشهادة);
3. Al-qasamah (القسم);
4. Al-Qarinah (القينة).³⁹

³⁸Ahmad Wardi Muslich, *Hukum Pidana Islam* (Cet. I; Jakarta: Sinar Grafika, 2005), h. 227.

³⁹Abdul Qadir Audah, *Al-Tasyri' al-Jinaiy al-Islamiy*, Juz II (Beirut, Dar al-Kitab al-'Arabi, [t.th]), h. 303.

Ketiga alat bukti tersebut selain *qasamah* (pengakuan, persaksian, dan *qarinah*) merupakan alat bukti yang banyak digunakan dalam *jarimah-jarimah hudud*. Perbedaan pendapat antara para ulama tersebut, hanya dalam alat bukti yang keempat, yaitu *qarinah*. Dalam uraian di bawah ini, akan diuraikan keempat jenis alat bukti tersebut, meskipun alat bukti yang paling kuat sebenarnya hanya dua, yaitu pengakuan dan persaksian. *Qasamah* sendiri juga termasuk alat bukti yang diperselisihkan, meskipun ulama-ulama dari kalangan mazhab yang empat telah menyepakatinya.

Berkaitan dengan kasus-kasus *cyber crime*, maka keempat alat bukti tersebut diperlukan untuk dapat mengungkapkan kebenaran dari suatu kejahatan yang terjadi di dunia *cyber*. Hal ini perlu ditegaskan, karena kasus-kasus yang menyangkut tindak pidana *cyber crime* berbeda dengan kejahatan konvensional. Lebih lanjut di paparkan alat-alat bukti yang berlaku dalam hukum pidana Islam sebagai berikut:

1. Pengakuan

Pengakuan (الإقرار) menurut bahasa adalah penetapan. Sedangkan menurut syarak, pengakuan didefinisikan sebagai berikut:

الإقرار... شرعاً هو الإخبار عن حقٍّ أو الاعتراف به

Artinya:

Pengakuan menurut syarak adalah suatu pernyataan yang menceritakan tentang sesuatu kebenaran atau mengakui kebenaran tersebut.⁴⁰

⁴⁰ *Ibid.*

Dasar hukum tentang *iqra* (pengakuan) ini terdapat dalam Alquran, sunah, dan ijma'. Adapun sumber dari Alquran tercantum dalam Q.S. al-Nisa/4: 135 sebagai berikut:

يَا أَيُّهَا الَّذِينَ ءَامَنُوا كُونُوا قَوَّامِينَ بِالْقِسْطِ شُهَدَاءَ لِلّٰهِ وَلَوْ عَلَىٰ أَنْفُسِكُمْ أَوِ الْوَالِدِينَ وَالْأَقْرَبِينَ ۚ إِن يَكُنْ غَنِيًّا أَوْ فَقِيرًا فَاللّٰهُ أَوْلَىٰ بِهِمَا ۖ فَلَا تَتَّبِعُوا هَوَىٰ ۖ أَنْ تَعْدِلُوا ۚ وَإِنْ تَلَوُّا أَوْ تُعْرَضُوا فَإِنَّ اللّٰهَ كَانَ بِمَا تَعْمَلُونَ خَبِيرًا .

Terjemahannya:

Wahai orang-orang yang beriman, jadilah kamu orang yang benar-benar penegak keadilan, menjadi saksi karena Allah walaupun terhadap dirimu sendiri atau ibu bapa dan kaum kerabatmu. Jika dia (yang terdakwa) kaya ataupun miskin, maka Allah lebih tahu kemaslahatannya (kebaikannya). Maka janganlah kamu mengikuti hawa nafsu karena ingin menyimpang dari kebenaran. Dan jika kamu memutar balikkan (kata-kata) atau enggan menjadi saksi, maka sesungguhnya Allah adalah Maha Mengetahui segala apa yang kamu kerjakan.⁴¹

Penyaksian seseorang atas dirinya sendiri ditafsirkan sebagai suatu pengakuan atas perbuatan yang dilakukannya.

Di samping dasar hukum tersebut, firman Allah dalam Q.S. Al-Imran/3: 81 juga menyebutkan sebagai berikut:

وَإِذْ أَخَذَ اللّٰهُ مِيثَاقَ النَّبِيِّينَ لَمَا آتَيْتُكُمْ مِنْ كِتَابٍ وَحِكْمَةٍ ثُمَّ جَاءَكُمْ رَسُولٌ مُّصَدِّقٌ لِّمَا مَعَكُمْ لَتُؤْمِنُنَّ بِهِ وَلَتَنْصُرُنَّهُ ۚ قَالَ أَأَقْرَرْتُمْ وَأَخَذْتُمْ عَلَىٰ ذَٰلِكُمْ إِصْرِي ۖ قَالُوا أَقْرَرْنَا ۖ قَالَ فَاشْهَدُوا ۚ وَأَنَا مَعَكُمْ مِنَ الشَّاهِدِينَ

⁴¹Departemen Agama RI., *Alquran dan Terjemahnya* (Bandung, PT Syaamil Cipta Media, 2004), h. 100.

Terjemahannya:

Dan (ingatlah), ketika Allah mengambil perjanjian dari para nabi: “Mana kala Aku memberikan kitab dan hikmah kepadamu lalu datang kepada kamu seorang rasul yang membenarkan apa yang ada pada kamu, niscaya kamu akan sungguh-sungguh beriman kepadanya dan menolongnya”. Allah berfirman: “Apakah kamu setuju dan menerima perjanjian dengan-Ku atas yang demikian itu?” Mereka menjawab: “Kami setuju”. Allah berfirman: “Kalau begitu bersaksilah (para nabi) dan Aku menjadi saksi bersama kamu.”⁴²

Sumber hukum dari sunah terdapat di dalam hadis Ma’iz yang datang kepada nabi mengakui perbuatannya, dan hadis tentang kisah al-‘Asif Nabi saw. bersabda:

... وَأَعْدِيَا أُنَيْسٍ لِرَجُلٍ مِّنْ أَسْلَمَ إِلَى امْرَأَةٍ هَذَا فَإِنْ اعْتَرَفَتْ فَارْجَمْهَا (متفق عليه)

Artinya:

...dan pergilah kamu hai Unais untuk memeriksa istrinya laki-laki ini, apabila ia mengaku (berzina) maka rajamlah dia (HR. Muttafaun ‘Alaih).⁴³

Di samping dasar hukum Alquran dan sunah, para ulama telah sepakat tentang keabsahan pengakuan, karena pengakuan merupakan suatu pernyataan yang dapat menghilangkan keraguan dari orang menyatakan pengakuan tersebut. Hal ini dimaksudkan bahwa orang yang berakal sehat tidak akan melakukan kebohongan yang mengakibatkan dapat merugikan dirinya. Karena itu, pengakuan lebih kuat dari pada persaksian, dan dapat digunakan sebagai alat bukti untuk semua jenis tindak pidana, termasuk *jarimah qisas* dan diat.

Pengakuan dalam konteks di atas tidak berlaku secara mutlak, akan tetapi terjadi secara normal. Hal ini dapat dilihat, apakah pengakuan hadir karena paksaan ataukah karena kerelaan sebagai wujud kesadaran terhadap kesalahan yang

⁴²*Ibid.*, h. 60.

⁴³Muhammad Ibn Ali al-Syaukani, *Nail al-Authar*, Juz VII (Beirut, Dar al-Fikr, [t.th.]), h. 249.

dilakukannya. Jika pengakuan dilakukan atas dasar kesadarannya, maka pengakuan lebih kuat dari kesaksian. Berbeda halnya apabila kondisi tidak normal, maka keseluruhan alat bukti termasuk saksi juga harus didalami untuk mendapatkan kebenaran yang sesungguhnya. Sebab seluruh alat bukti berpeluang untuk dimanipulasi sehingga bukti-bukti tersebut harus diuji kevalidannya secara proporsional.

Pengakuan hanya berlaku untuk orang yang bersangkutan dan tidak berlaku untuk orang lain. Apabila A mengaku membunuh B dengan dibantu oleh C, sedangkan C mengingkarinya, maka pengakuan itu hanya berlaku untuk A dan tidak berlaku untuk C. Ketentuan ini didasarkan kepada sunah fi'liyah berkaitan dengan jarimah zina berikut:

عَنْ سَهْلِ بْنِ سَعْدٍ أَنَّ رَجُلًا جَاءَ إِلَى النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ فَقَالَ إِنَّهُ قَدْ زَنَى بِامْرَأَةٍ سَمَّاها فَرَسَلَهُ النَّبِيُّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ إِلَى الْمَرْأَةِ فَدَعَاها فَسَالَهَا عَمَّا قَالَتْ فَأَنْكَرَتْ فَحَدَّثَهُ وَتَرَكَهَا (رواه أحمد وأبو داود)

Artinya:

Dari Sahl Ibn Sa'ad bahwa seorang laki-laki telah datang kepada Nabi saw. kemudian ia mengatakan bahwa ia telah berzina dengan seorang perempuan yang ia sebutkan namanya. Nabi saw. kemudian mengutus seorang sahabat untuk memanggil perempuan tersebut. Nabi saw. kemudian bertanya kepada perempuan tersebut mengenai apa yang dikatakan oleh laki-laki tadi, tetapi perempuan tersebut mengingkarinya. Akhirnya, Nabi saw. menghukum laki-laki tersebut dan membebaskan perempuan yang tidak mengaku (HR. Ahmad dan Abu Daud).⁴⁴

Pengakuan yang dapat diterima sebagai alat bukti adalah pengakuan yang jelas, terperinci, dan pasti, sehingga tidak bisa ditafsirkan lain kecuali perbuatan pidana yang dilakukannya. berbagai aspek yang berkaitan dengan tindak pidana

⁴⁴*Ibid.*, h. 273-274.

pembunuhan misalnya, seperti caranya, alatnya, motifnya, tempat, dan waktunya harus diungkapkan secara jelas oleh orang yang mengaku melakukan perbuatan tersebut. Apabila pengakuan tersebut hanya diceritakan secara globalnya saja, maka pengakuan tersebut belum bisa diterima sebagai alat bukti yang kuat dan meyakinkan.

Kejelasan dan rincian dari pengakuan tersebut didasarkan kepada sunah Rasulullah saw. ketika beliau menginterogasi Ma'iz yang mengaku berzina dan mengulangi pengakuannya itu sebanyak empat kali. Dalam interogasinya Nabi saw. menanyakan sebagai berikut:

لَعَلَّكَ قَبْلَتْ أَوْ غَمَزْتَ أَوْ نَظَرْتَ، قَالَ: لَا، يَا رَسُولَ اللَّهِ (رواه البخاري)

Artinya:

Barangkali engkau hanya menciumnya, atau meremas-remasnya, atau hanya memandangnya? Ma'iz menjawab: Tidak, ya Rasulullah (HR. Bukhari)⁴⁵

Di samping itu, syarat yang lain untuk sahnya pengakuan adalah bahwa pengakuan harus benar dan tidak dipaksa (terpaksa). Pengakuan yang demikian harus timbul dari orang yang berakal dan memiliki kebebasan (pilihan). Dengan demikian, pengakuan yang datang dari orang gila atau hilang akalnya, dan yang dipaksa hukumnya tidak sah dan tidak dapat diterima.

Apabila orang yang menyatakan pengakuan, lalu ia menarik kembali pengakuannya, maka penarikan dan pencabutan pengakuan tersebut dapat diterima apabila tindak pidana yang semula diakuinya itu berkaitan dengan hak Allah yang

⁴⁵Muhammad Ibn Ismail al-Kahlani, *Subl al-Salam*, Juz (Mesir: Maktabah Mushtafa al-Baby al-Halaby, 1960), h. 8.

gugur karena adanya *syubhat*. Adapun tindak pidana yang berkaitan dengan hak manusia atau hak Allah yang tidak gugur karena syubhat, seperti zakat dan kifarat maka penarikan atau pencabutan pengakuan tersebut tidak dapat diterima. Apabila seseorang mengaku berbuat zina tetapi kemudian ia menarik pengakuannya, maka ia tidak dituntut karena pengakuannya itu. Akan tetapi, apabila ia mengaku membunuh orang atau melukainya, kemudian ia mencabut pengakuannya maka ia tetap dituntut karena tindakan yang dilakukannya berkaitan dengan hak manusia yang tidak bisa digugurkan kecuali dengan kerelaan pemiliknya.

2. Persaksian

Pengertian persaksian, sebagaimana dikemukakan oleh Wahbah Zuhaili adalah sebagai berikut:

وَهِيَ إِخْبَارٌ صَادِقٌ لِاثْبَاتٍ حَقٌّ بِلَفْظِ الشَّهَادَةِ فِي مَجْلِسِ الْقَضَاءِ

Artinya:

Persaksian adalah suatu pemberitahuan (pernyataan) yang benar untuk membuktikan suatu kebenaran dengan lafaz syahadat di depan pengadilan.⁴⁶

Penggunaan saksi sebagai alat pembuktian untuk suatu *jarimah* merupakan cara yang lazim dan umum. Karenanya persaksian merupakan cara pembuktian yang sangat penting dalam mengungkapkan suatu *jarimah*.

Dasar hukum untuk persaksian sebagai alat bukti terdapat dalam Alquran dan sunah. Dalam Alquran sebagaimana disebutkan dalam Q.S. al-Baqarah/2: 282 sebagai berikut:

⁴⁶Wahbah Zuhaili, *Al-Fiqh al-Islami wa Adillatuhu*, Juz VI (Damaskus: Dar al-Fikr, 1989), h. 388.

وَأَسْتَشْهِدُوا شَهِيدَيْنِ مِنْ رِجَالِكُمْ ۖ فَإِنْ لَمْ يَكُونَا رَجُلَيْنِ فَرَجُلٌ وَامْرَأَتَانِ مِمَّنْ تَرْضَوْنَ مِنَ الشُّهَدَاءِ أَنْ تَضِلَّ إِحْدَاهُمَا فَتُذَكِّرَ إِحْدَاهُمَا الْأُخْرَىٰ

Terjemahannya:

... Dan persaksikanlah dengan dua orang saksi dari orang-orang lelaki (di antara kamu). Jika tidak ada (saksi) dua orang laki-laki, maka (boleh) seorang laki-laki dan dua orang perempuan di antara orang-orang yang kamu sukai dari para saksi (yang ada), agar jika seorang lupa maka yang seorang lagi mengingatkannya ...⁴⁷

Dalam QS. al-Talaq/65: 2 juga disebutkan sebagai berikut:

وَأَشْهِدُوا ذَوَيْ عَدْلٍ مِّنكُمْ وَأَقِيمُوا الشَّهَادَةَ لِلَّهِ

Terjemahannya:

... dan persaksikanlah dengan dua orang saksi yang adil di antara kamu dan hendaklah kamu tegakkan kesaksian itu karena Allah...⁴⁸

Sumber dari sunah antara lain tercantum dalam hadis Amr Ibn Syu'aib:

وَعَنْ عَمْرِو بْنِ شُعَيْبٍ عَنْ أَبِيهِ عَنْ جَدِّهِ أَنَّ ابْنَ مُحِيصَةَ الْأَصْغَرَ أَصْبَحَ قَتِيلًا عَلَىٰ أَبَوَابِ خَيْبَرَ فَقَالَ رَسُولُ اللَّهِ صَلَّيْهُ عَلَيْهِ وَسَلَّمَ أَقِمُوا شَاهِدَيْنِ عَلَىٰ مَنْ قَتَلَهُ أَدْفَعُهُ إِلَيْكُمْ بِرُمَّتِهِ... (رواه النسائي)

Artinya:

Dari 'Amr ibn Syu'aib dari ayahnya dari kakeknya, bahwa anaknya Muhaishah yang paling kecil ditemukan terbunuh di pintu Khaibar maka Rasulullah saw. bersabda: "Ajukanlah dua orang saksi atas orang yang membunuhnya, nanti saya berikan kepadamu tambang untuk mengkisasnya ... (Hadis Riwayat Nasa'i).⁴⁹

⁴⁷Departemen Agama RI., *op. cit.*, h. 48.

⁴⁸*Ibid.*, h. 558.

⁴⁹Asy-Syaukam, V11, *op. cit.*, h. 181-182.

Dalam pembuktian tindak pidana pembunuhan dan pelukaan (penganiayaan), para fukaha membedakan antara *jarimah* yang hukumannya badaniah, seperti *qisās* dera, dan lain-lain dengan *jarimah* yang hukumannya maliah, seperti diat atau ganti rugi.

a. *Jarimah* yang Hukumannya Badaniah

Jarimah yang hukumannya badaniah adakalanya *qisās* dan ada kalanya takzir. Untuk *jarimah* yang hukumannya *qisās* menurut jumhur fukaha, pembuktiannya harus dengan dua orang saksi laki-laki, dan tidak boleh dengan seorang saksi laki-laki dan dua perempuan, atau seorang saksi laki-laki ditambah sumpahnya korban. Ketentuan ini berlaku baik dalam *qisās* jiwa maupun bukan jiwa, kecuali pendapat Imam Malik. Menurut Imam Malik pembuktian dengan dua orang saksi laki-laki hanya berlaku dalam *qisās* atas jiwa saja. Adapun untuk *qisās* atas bukan jiwa, pembuktiannya bisa dengan seorang saksi laki-laki dan sumpahnya korban, dengan menggunakan dasar *istihṣān*. Sedangkan menurut Imam al-Auza'i dan al-Zuhri, pembuktian untuk *jarimah* yang hukumannya maliah, yaitu bisa dengan dua orang saksi laki-laki atau seorang saksi laki-laki dan dua orang perempuan.⁵⁰

Untuk *jarimah* yang hukumannya takzir badaniah bersama-sama dengan *qisās* maka pembuktiannya sama dengan *jarimah* yang mewajibkan hukuman *qisās*. Adapun *jarimah* yang mewajibkan hukuman takzir badaniah tanpa *qisās* maka menurut Imam Syafi'i dan Imam Ahmad, pembuktiannya sama dengan *jarimah* yang hukumannya *qisās* yaitu harus dengan dua orang saksi laki-laki yang adil. Hal ini karena hukuman badan itu merupakan hukuman yang cukup mengkhawatirkan, sehingga pembuktiannya harus hati-hati. Sedangkan menurut Imam Malik, untuk

⁵⁰ Abd At-Qadir Audah, II, *op. cit.*, h. 315-316.

pembuktian *jarimah qisas* selain jiwa bisa dengan dua orang saksi laki-laki dan sumpahnya korban, dan hukuman yang dijatuhkan di samping *qisas* ditambah dengan hukuman takzir. Menurut Imam Abu Hanifah, untuk membuktikan jarimah yang hukumannya takzir bisa digunakan dua saksi laki-laki yang salah satunya adalah korban, atau seorang saksi laki-laki dan dua orang perempuan. Bahkan menurut kedua muridnya dalam kasus ini, pembuktiannya cukup dengan seorang saksi laki-laki yang adil, atau dengan persaksian penuntut (korban) ditambah dengan keengganan bersumpahnya terdakwa, atau bahkan cukup dengan pengetahuan hakim (*'ilmul qadi*).⁵¹

b. *Jarimah* yang Hukumannya Maliah

Menurut Imam Syafi'i dan Imam Ahmad, pembuktian untuk *jarimah* yang hukumannya maliah, seperti diat atau ganti rugi, bisa dengan dua orang saksi laki-laki, atau seorang laki-laki dan dua orang perempuan, atau seorang laki-laki dan sumpahnya penuntut (korban) atau keengganan bersumpahnya terdakwa. Malikiyah berbeda pendapatnya dengan Imam Syafi'i dan Imam Ahmad. Mereka (Malikiyah) membolehkan pembuktian untuk *jarimah* yang hukumannya maliah dengan saksi dua orang wanita ditambah dengan sumpahnya penuntut, sedangkan Imam Syafi'i dan Imam Ahmad tidak membolehkannya. Alasan mereka (Malikiyah) adalah bahwa dua orang perempuan dapat menggantikan seorang laki-laki dalam kedudukannya sebagai saksi dalam masalah harta benda. Oleh karena itu, maka dalam hukuman maliah dua orang perempuan juga bisa digunakan sebagai saksi untuk pembuktian tindak pidananya. Sedangkan menurut Imam Abu Hanifah dan pengikutnya, untuk pembuktian tindak pidana yang hukumannya maliah dapat digunakan dua orang

⁵¹*Ibid.*, h. 317.

saksi laki-laki, atau seorang laki-laki dan dua orang perempuan. Mereka tidak membolehkan digunakannya seorang saksi laki-laki ditambah dengan sumpah atau dua orang perempuan ditambah dengan sumpah, karena hal itu berarti menambah-nambah nas yang terecantum dalam surat al-Baqarah ayat 282.⁵² Di samping itu, Rasulullah saw. menyatakan dalam hadisnya:

... وَلَلْبَيْهَقَى بِإِسْنَادٍ صَحِيحٍ: الْبَيِّنَةُ عَلَى الْمُدَّعَى وَالْيَمِينُ عَلَى مَنْ أَنْكَرَ

Artinya:

...Dan diriwayatkan oleh Al-Baihaqi dengan sanad yang sahih: “Keterangan (saksi) adalah hak penuntut, sedangkan sumpah adalah haknya terdakwa (orang yang ingkar).⁵³

Ibn al-Qayyim berpendapat bahwa tindak pidana yang hukumannya maliah dapat dibuktikan dengan seorang saksi tanpa diperkuat dengan sumpah, apabila hakim mempercayai dan meyakini keterangan yang disampaikan oleh saksi tersebut.⁵⁴ Apabila hakim tidak meyakini keterangan saksi, karena keterangannya meragukan maka hakim dapat menolaknya.

Para fukaha secara umum juga membolehkan pembuktian dengan seorang saksi laki-laki atau seorang perempuan dalam keadaan darurat, baik untuk membuktikan substansi tindak pidana itu sendiri atau pengaruh dan akibat dari tindak pidana tersebut. Contoh untuk bagian pertama seperti kesaksian seorang guru atas jarimah yang terjadi di lingkungan sekolah oleh anak-anak. Sedangkan contoh

⁵²*Ibid.*, h. 318-319.

⁵³Al-Kahlani, IV, *op. cit.*, h. 132.

⁵⁴Ibn al-Qayyim al-Jauziah, *I'lam al-Muwaqqi'in al-Rabbil 'Alamin*, Juz I ([t.tp], Dar al-Fikr, 1877), h. 96.

untuk bagian kedua seperti kesaksian seorang dokter bahwa pemukulan mengakibatkan hilangnya manfaat salah satu anggota badan korban.⁵⁵

Pada akhirnya, kunci untuk diterimanya kesaksian adalah adanya keyakinan hakim. Apabila keterangan para saksi tidak seragam, atau bahkan bertentangan antara saksi yang satu dengan saksi yang lain maka kesaksian yang demikian tentu saja meragukan dan hakim sebagai pengambil keputusan tentu tidak yakin dan menolak kesaksian tersebut.

3. *Qasamah*

a. Definisi *Qasamah*

Qasamah dalam arti bahasa adalah (الْحُسْنُ وَالْجَمَالُ) yang artinya bagus dan indah; (الْيَمِينُ) yang artinya sumpah.⁵⁶

Sedangkan menurut arti istilah, *qasamah* didefinisikan sebagai berikut.

وَالْمُرَادُ بِالْقَسَامَةِ هَهُنَا الْإِيمَانُ الْمَكْرَرُ فِي دَعْوَى الْقَتْلِ

Artinya:

Adapun yang dimaksud dengan *qasamah* di sini adalah sumpah yang diulang-ulang dalam dakwaan (tuntutan) pembunuhan.⁵⁷

Hanafiyyah mendefinisikan *qasamah* sebagai berikut:

... فِي عُرْفِ الشَّرْعِ تُسْتَعْمَلُ فِي الْيَمِينِ بِاللَّهِ تَبَارَكَ وَتَعَالَى بِسَبَبِ مَخْصُوصٍ وَعَدَدٍ مَخْصُوصٍ وَعَلَى شَخْصٍ مَخْصُوصٍ وَهُوَ الْمُدَّعَى عَلَيْهِ عَلَى وَجْهِ مَخْصُوصٍ.

⁵⁵ Abd. Al-Qadir Audah, II, *op. cit.*, h. 320-321.

⁵⁶ Ibrahim Unais, *et al.*, *Al-Mu'jam al-Wasit*, Juz II ([t.tp]: Dar Ihya' al-Turats, [t.th]), h. 735.

⁵⁷ Abdullah Ibn Qudamah Al-Maqdisi, *Al-Mugni*, Juz VIII ([t.tp]: Dar al-Manar, [t.tp]), h. 64.

Artinya:

Dalam istilah syarak, *qasamah* digunakan untuk arti sumpah dengan nama Allah SWT karena adanya sebab tertentu, dengan bilangan tertentu, untuk orang tertentu yaitu si terdakwa dan menurut cara tertentu.⁵⁸

Dari definisi tersebut dapat dipahami bahwa *qasamah* adalah sumpah yang diulang-ulang. Hanya saja siapa yang bersumpah masih diperselisihkan oleh para fukaha. Menurut Hanafiyah, sumpah dilakukan oleh penduduk tempat ditemukannya korban, sedangkan jumhur ulama menyatakan sumpah dilakukan oleh keluarga korban. Atas dasar itu, Abdul Qadir Audah dan juga Wahbah Zuhaili membuat definisi yang merangkum kedua pendapat tersebut dengan mengatakan:

وَمَعْنَى الْقَسَامَةِ فِي اصْتِلَاحِ الْفُقَهَاءِ الْإِيمَانُ الْمَكْرَرُ فِي دَعْوَى الْقَتْلِ يَقْسِمُ بِهَا أَوْلِيَاءُ الْقَتِيلِ لِاثْبَاتِ الْقَتْلِ عَلَى الْمُتَّهِمِ أَوْ يَقْسِمُ بِهَا الْمُتَّهِمُ عَلَى نَفْيِ الْقَتْلِ عَنْهُ.

Artinya:

Arti *qasamah* menurut istilah para fukaha adalah sumpah yang diulang-ulang di dalam dakwaan (tuntutan) pembunuhan, yang dilakukan oleh wali (keluarga si terbunuh) untuk membuktikan pembunuhan atas tersangka, atau dilakukan oleh tersangka untuk membuktikan bahwa ia tidak melakukan pembunuhan.⁵⁹

b. Dasar Hukum Disyariatkannya *Qasamah*

Qasamah merupakan salah satu cara pembuktian yang berlaku pada zaman jahiliah. Setelah Islam datang, nabi mengakui dan menetapkan (qasamah) sebagai salah satu alat bukti yang sah untuk tindak pidana pembunuhan. Hal ini dijelaskan dalam beberapa hadis Nabi.

⁵⁸Ala al-Din al-Kasani, Kitab Badai' al-Shanai' fi Tartib al-Syarak (Beirut: Dar al-Fikr, 1996), h. 422.

⁵⁹Abd At-Qadir Audah, II, *op. cit.*, h. 321-322; Wahbah Zuhaili, *op. cit.*, h. 393-394.

1) Hadis nabi yang diriwayatkan oleh Abi Salamah

عَنْ أَبِي سَلَمَةَ بْنِ عَبْدِ الرَّحْمَنِ وَسُلَيْمَانَ بْنِ يَسَارٍ عَنْ رَجُلٍ مِنْ أَصْحَابِ النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ الْأَنْصَارِ، أَنَّ النَّبِيَّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ أَقْرَأَ الْقَسَامَةَ عَلَى مَا كَانَتْ عَلَيْهِ فِي الْجَاهِلِيَّةِ (رواه أحمد ومسلم والنسائي)

Artinya:

Dari Abi Salamah ibn Abd Al-Rahman dan Sulaiman ibn Yasar dari seorang laki-laki sahabat Nabi saw. kelompok Anshar, bahwa sesungguhnya Nabi saw. menetapkan *qasamah* (sebagai alat bukti) sebagaimana yang berlaku di zaman jahiliah. (Hadis riwayat Ahmad, Muslim, dan Nasa'i).⁶⁰

2) Hadis Nabi yang diriwayatkan oleh Sahl ibn Abi Hatsmah

وَعَنْ سَهْلِ بْنِ أَبِي حَثْمَةَ قَالَ: انْطَلَقَ عَبْدُ اللَّهِ بْنُ سَهْلٍ وَمُحَيْصَةُ ابْنُ مَسْعُودٍ إِلَى خَيْبَرَ وَهُوَ يَوْمَئِذٍ صَلَحٌ فَتَفَرَّقَا، فَاتَى مُحَيْصَةُ إِلَى عَبْدِ اللَّهِ بْنِ سَهْلٍ وَهُوَ يَتَشَحَّطُ فِي دَمِهِ قَتِيلًا فَدَفَنَهُ، ثُمَّ قَدِمَ الْمَدِينَةَ فَانْطَلَقَ عَبْدُ الرَّحْمَنِ بْنُ سَهْلٍ مُحَيْصَةَ وَحَوَيْصَةَ ابْنَا مَسْعُودٍ إِلَى النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ فَذَهَبَ عَبْدُ الرَّحْمَنِ يَتَكَلَّمُ، فَقَالَ: كَبِيرٌ وَهُوَ أَحَدُ الْقَوْمِ فَسَكَتَ فَتَكَلَّمَا، قَالَ: أَتَخْلِفُونَ وَتَسْتَحِقُونَ قَاتِلَكُمْ أَوْصَابَكُمْ، فَقَالُوا: وَكَيْفَ نَخْلِفُ وَلَمْ نَشْهَدْ وَلَمْ نَر؟ قَالَ: فَتَبَرُّكُمْ يَهُودُ بَخْمَسِينَ يَمِينًا، فَقَالُوا: كَيْفَ نَأْخُذُ بِإِيمَانِ قَوْمٍ كُفَّارٍ؟ فَعَقَلَهُ النَّبِيُّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ مِنْ عِنْدِهِ (رواه الجماعة)

Artinya:

Dari Sahl ibn Abi Hasamah ia berkata: “Abdullah ibn Sahal dan Muhaishah ibn Mas'ud pergi ke Khaibar yang waktu itu dalam keadaan damai; kemudian keduanya berpisah. Setelah itu Muhaishah mendatangi Abdullah ibn Sahal yang mati dengan berlumuran darah, lalu ia menguburkannya, dan setelah itu ia kembali ke Madinah. Abdurrahman ibn Sahal, dan Muhaishah serta

⁶⁰Muhammad ibn Ali al-Syaukani, VII, *op. cit.*, h. 183.

Huwaishah keduanya anak Ibn Mas'ud pergi menghadap Nabi saw. Maka Abdurrahman memulai pembicaraan tetapi nabi berkata: Panggillah orang yang lebih tua umurnya darimu, dan dialah yang berbicara mewakili kaummu maka Abdurrahman diam, dan berbicaralah dua orang bersaudara (Muhaisah dan Huwaisah). Nabi kemudian berkata: 'Apakah kalian mau bersumpah dan kalian berhak terhadap pembunuh saudaramu?' Mereka berkata: 'Bagaimana kami bersumpah, padahal kami tidak menyaksikan dan tidak pula melihat (peristiwa pembunuhan tersebut)?' Nabi berkata: 'Kalian bisa meminta kepada kaum Yahudi (Khaibar) untuk bersumpah lima puluh kali.' Mereka berkata lagi: 'Bagaimana kami akan meminta sumpah dari kaum kafir?' Akhirnya Nabi saw. membayar diat untuk si korban dari harta nabi sendiri. (Hadis riwayat jama'ah)⁶¹

Dari kedua hadis tersebut, jelaslah bahwa *qasamah* pernah dilaksanakan oleh nabi, meskipun pada awalnya *qasamah* itu merupakan suatu tradisi yang dilakukan oleh orang-orang Arab zaman jahiliyah, ketika mereka menghadapi kasus pembunuhan yang tidak ada bukti-bukti, baik saksi maupun pengakuan. Atas dasar hadis-hadis tersebut, jumhur ulama, seperti ulama mazhab empat, Zahiriyah, dan Syi'ah berpendapat bahwa *qasamah* merupakan salah satu cara pembuktian yang sah dan diakui untuk tindak pidana pembunuhan.⁶² Akan tetapi, beberapa fukaha yang lain, seperti Salim ibn Abdullah, Abu Qalabah, Umar ibn Abdul Aziz, Al-Hakam ibn Utaibah, Qatadah, Sulaiman ibn Yasar, Ibrahim ibn Aliyah, dan Muslim ibn Khalid berpendapat bahwa *qasamah* tidak boleh dijadikan alat bukti untuk tindak pidana pembunuhan. Alasannya adalah karena *qasamah* menyimpang dari prinsip-prinsip pokok syariat Islam, yang meliputi berikut ini:

- 1) Seseorang tidak boleh bersumpah kecuali atas apa yang ia ketahui secara pasti dan ia saksikan dengan mata kepalanya sendiri. Sedangkan dalam *qasamah*, wali korban sama sekali tidak mengetahui dan tidak menyaksikan pembunuhan, karena

⁶¹*Ibid.*, h. 183-184.

⁶²Abd al-Qadir Audah, II, *op. cit.*, h. 324.

tindak pidana pembunuhan tersebut terjadi di tempat yang jauh dari tempat tinggal mereka (keluarga korban).

- 2) Pembuktian atau keterangan adalah hak penuntut, sedangkan sumpah adalah hak terdakwa.
- 3) Mengenai hadis Sahal yang digunakan sebagai dalil oleh kelompok pertama, kelompok kedua ini tidak menganggapnya sebagai dalil untuk qasamah, melainkan sekedar upaya memperlunak kebiasaan-kebiasaan zaman jahiliah, untuk kemudian dibatalkan secara berangsur-angsur, sedikit demi sedikit.⁶³

Alasan dari pendapat kedua ini dibantah oleh kelompok pertama dengan argumentasi, bahwa qasamah ditetapkan berdasarkan hadis yang khusus, sehingga tidak bisa diabaikan dengan dalil yang umum, melainkan justru men-takhsiskannya. Hal ini dimaksudkan untuk memelihara keselamatan jiwa dan sebagai pencegahan terhadap pelaku (pelanggar hukum).

c. Tujuan Disyariatkannya *Qasamah*

Qasamah disyariatkan dalam rangka memelihara jiwa, sehingga dalam keadaan bagaimanapun pembunuhan itu harus tetap diselesaikan, dibuktikan, dan ditetapkan hukumannya. Dengan demikian, *qasamah* merupakan suatu jalan keluar untuk menyelesaikan suatu kasus pembunuhan, di mana tidak terdapat bukti berupa saksi atau pengakuan.

Dalam rangka memelihara jiwa ini, Imam Ahmad berpendapat bahwa seseorang, yang meninggal akibat berdesak-desakan dalam salat atau tawaf, diatnya tetap harus dibayar dari Baitul Mal, seperti yang pernah dilakukan oleh Nabi dalam hadis Sahal yang telah dikemukakan di atas. Pendapat ini juga dikemukakan oleh

⁶³Wahbah Zuhaili, *op. cit.*, h. 397.

Sayidina Umar dan Sayidina Ali. Diriwayatkan oleh Sa'id dari Ibrahim bahwa seseorang terbunuh di dalam kerumunan manusia yang berdesak-desakan di 'Arafah. Kemudian keluarganya datang menghadap Umar, lalu Umar berkata: "Buktikan siapa yang membunuhnya?" Maka berkata Saydina Ali: "Ya Amirul Mukminin, tidak akan dialirkan darah seorang muslim, andai kata saya tahu siapa pembunuhnya, kalau tidak maka bayarlah diatnya dari Baitul Mal!"⁶⁴

Menurut Hanafiyah, *qasamah* disyariatkan untuk menanggulangi kelalaian warga tempat ditemukannya korban dalam menjaga dan memelihara wilayahnya dari tindakan-tindakan kriminal yang dilakukan, baik oleh penduduk setempat maupun oleh pihak luar. Akibat kelalaian mereka dalam mengamankan wilayahnya, mereka dibebani kewajiban harus melakukan *qasamah* dan sekaligus membayar diat, karena menurut Imam Abu Hanifah, mereka baik sebagai individu maupun kelompok dianggap membunuh korban, karenanya mereka harus bertanggung jawab.⁶⁵

d. Penggunaan *Qasamah*

Para ulama sepakat bahwa *qasamah* hanya digunakan untuk tindakan pembunuhan, bukan yang lainnya. Hanya saja mengenai kapan digunakannya *qasamah*, para ulama berbeda pendapat. Menurut Imam Abu Hanifah, *qasamah* digunakan apabila pelaku (pembunuh) tidak diketahui. Apabila pelakunya diketahui, maka pembuktiannya tidak menggunakan *qasamah*, melainkan menggunakan cara-cara pembuktian biasa.⁶⁶

⁶⁴Abd al-Qadir Audah, II, *op. cit.*, h. 327.

⁶⁵*Ibid.*, h. 328.

⁶⁶Al-Kasani, VII, *op. cit.*, h. 425.

Menurut Imam Malik, Imam Syafi'i, dan Imam Ahmad, *qasamah* digunakan apabila pelaku (pembunuh) diketahui karena ada tanda dan petunjuk yang mengarah kepadanya. Apabila pembunuh tidak diketahui, maka menurut mereka (jumhur) *qasamah* tidak dapat diberlakukan.⁶⁷

Qarinah atau petunjuk (الْوُتُّ) didefinisikan oleh Imam Malik dan Imam Syafi'i sebagai berikut:

وَالْوُتُّ هُوَ مَا يَنْشَأُ عَنْ غَلَبَةِ الظَّنِّ بِصِدْقِ الْمُدَّعِي، أَوْ هُوَ قَرِينَةٌ تَوَقَّعُ فِي الْقَلْبِ صِدْقَ الْمُدَّعِي.

Artinya:

Laus adalah suatu keadaan yang timbul dari dugaan yang kuat atas kebenaran penuntut, atau *laus* adalah suatu *qarinah* (petunjuk) yang masuk ke dalam hati tentang kebenaran penuntut.⁶⁸

Dari definisi tersebut dapat dipahami bahwa *laus* adalah suatu petunjuk yang memperkuat dugaan penuntut bahwa seseorang betul membunuh korban. Contohnya, seperti adanya jasad korban di halaman rumah musuhnya, atau terlihatnya tersangka di dekat kepala korban, dan di tangannya ada pisau yang terhunus.

Menurut Imam Ahmad dalam riwayat yang *marjuh* (lemah), *laus* adalah permusuhan yang nyata antara korban dengan terdakwa. Contohnya seperti permusuhan antara kaum Anshar dengan Yahudi Khaibar, atau antara pencuri dengan polisi yang menangkapnya. Sedangkan menurut riwayat yang *rajih* (kuat), *laus* adalah sesuatu yang memperkuat dugaan tentang kebenaran tuduhan penuntut. Contohnya seperti permusuhan yang telah disebutkan tadi, atau seperti bercerai--

⁶⁷ Ibn Qudamah, VIII, *op. cit.*, h. 65-66; Abd. Al-Qadir Audah, II, *op. cit.*, h. 329.

⁶⁸ Abd. Al-Qadir Audah, II, *Ibid.*, h. 330.

berainya sekelompok orang dari tempat terbunuhnya korban, atau ditemukannya seseorang di dekat korban, dan ia memegang pisau yang berlumuran darah.⁶⁹

Dari uraian tersebut di atas dapat diambil intisari bahwa *qasamah* menurut Imam Malik dan Imam Syafi'i diberlakukan, apabila pelaku pembunuhan diketahui tetapi tidak ada bukti yang kuat bahwa dialah yang membunuh korban. Namun demikian, ada *laus* (petunjuk) yang memperkuat bahwa dialah pembunuhnya. Dari pengertian ini dapat dipahami bahwa *qasamah* menurut mereka (Imam Malik dan Imam Syafi'i) digunakan untuk membuktikan tindak pidana yang dilakukan oleh pelaku. Sedangkan menurut Imam Abu Hanifah, *qasamah* digunakan apabila jasad korban ditemukan di tempat tertentu tetapi pelakunya sama sekali tidak diketahui. Karena itu, *qasamah* diberikan kepada penduduk tempat ditemukannya korban untuk membuktikan bahwa mereka tidak melakukan pembunuhan. Akan tetapi, mereka tetap dibebani kewajiban membayar diat, karena pembunuhan terjadi akibat keteledoran dan kelalaian mereka dalam menjaga keamanan wilayahnya.

e. Syarat-Syarat *Qasamah*

Qasamah tidak dapat dipergunakan sebagai alat bukti kecuali apabila syarat-syaratnya telah terpenuhi. Syarat-syarat tersebut adalah sebagai berikut:

- 1) Kematian yang dialami oleh korban merupakan akibat tindak pidana pembunuhan, baik karena pelukaan, pemukulan, pencekikan, maupun lainnya. Apabila tidak ada bekas-bekas atau tanda-tanda pembunuhan, maka tidak ada *qasamah* dan tidak ada diat.
- 2) Jumhur ulama selain Hanafiyah mensyaratkan adanya *laus* atau petunjuk yang mengarah kepada pelaku pembunuhan, seperti ditemukannya jasad korban di

⁶⁹*Ibid.*

halaman rumah musuhnya. Apabila tidak ada *laus*, maka tidak ada *qasamah*. Akan tetapi, Imam Abu Hanifah tidak mensyaratkan adanya *laus*, melainkan cukup ditemukannya mayat dan ada bekas pembunuhan.⁷⁰

- 3) Hanafiyah mensyaratkan terdapatnya sebagian besar dari jasad korban di tempat kejadian. Apabila yang ditemukan hanya satu anggota badan saja, tidak ada *qasamah* dan tidak ada diat. Apabila terdapat separuh badan berikut kepalanya maka berlaku *qasamah* dan diat. Akan tetapi, apabila hanya ditemukan kepalanya saja, maka tidak ada *qasamah* dan tidak ada diat. Sedangkan ulama yang lain tidak mensyaratkan hal ini.⁷¹
- 4) Imam Abu Hanifah mensyaratkan bahwa pembunuh tidak diketahui. Apabila pembunuh diketahui, maka tidak ada *qasamah*. Akan tetapi menurut Imam Malik, Imam Syafi'i, dan Imam Ahmad untuk diberlakukannya *qasamah*, justru pembunuh harus diketahui berdasarkan adanya petunjuk (*laus*). Apabila pembunuh tidak diketahui, maka *qasamah* tidak dapat digunakan.⁷²
- 5) Keluarga korban mengajukan tuntutan kepada tersangka.
- 6) Tuntutan yang diajukan oleh para keluarga korban tidak boleh bertentangan antara yang satu dengan yang lain. Misalnya sebagian wali (keluarga) menuntut bahwa pembunuhnya A, tetapi keluarga yang lain menyatakan bahwa pembunuhnya B. Jika pertentangan dalam tuntutan itu terjadi, maka *qasamah* tidak bisa digunakan.

⁷⁰*Ibid.* h. 337.

⁷¹*Ibid.*

⁷²*Ibid.*

- 7) Tersangka mengingkari perbuatan pembunuhan tersebut. Apabila pelaku pembunuhan mengakui perbuatannya maka *qasamah* tidak dapat digunakan, karena sudah ada alat bukti pengakuan.
- 8) Imam Abu Hanifah mensyaratkan adanya permintaan agar kasus pembunuhan tersebut dibuktikan dengan *qasamah*. Hal ini karena *qasamah* itu merupakan sumpah dan sumpah adalah hak penuntut yang dapat dipenuhi dengan permintaannya. Itulah sebabnya dalam *qasamah*, kesempatan pertama diberikan kepada keluarga korban, karena sumpah adalah hak mereka. Mereka berhak memilih dan menentukan orang-orang yang diduga sebagai tersangka pelaku pembunuhan dan meminta keluarga mereka yang baik-baik untuk bersumpah.⁷³
- 9) Imam Abu Hanifah juga mensyaratkan bahwa tempat mayat korban ditemukan adalah milik seseorang atau dalam kekuasaan seseorang. Apabila tempat (tanah) tersebut bukan milik seseorang atau bukan dalam kekuasaan seseorang, maka tidak ada *qasamah* dan tidak ada hukuman diat. Apabila mayat korban berada di tempat yang digunakan untuk kepentingan umum, maka tidak wajib *qasamah*, tetapi diat wajib dibayar dari Baitul Mal.⁷⁴

f. Cara Pelaksanaan *Qasamah*

Qasamah adalah suatu cara pembuktian dengan menggunakan sumpah yang dilakukan (diucapkan) oleh lima puluh orang. Akan tetapi kepada siapa sumpah itu diberikan pertama kali, apakah kepada penuntut atau terdakwa, para ulama berbeda pendapat.

⁷³*Ibid.*, h. 338.

⁷⁴Wahbah Zuhaili, VI, *op. cit.*, h. 402.

1) Menurut Hanafiyah, sumpah diberikan pertama kali kepada terdakwa, yaitu penduduk tempat ditemukannya mayat korban. Hal ini karena sumpah itu harus dilakukan oleh terdakwa yang dipilih dan ditunjuk oleh keluarga korban. penuntut (keluarga korban) memilih orang-orang yang diduga sebagai pelaku pembunuhan, dan mereka sebanyak lima puluh orang, masing-masing bersumpah, dengan mengatakan:

وَاللّٰهُ مَا قَتَلْتَنَاهُ وَلَا عَلِمْنَاهُ قَاتِلًا.

Artinya:

Demi Allah, saya tidak membunuhnya, dan saya tidak tahit siapa pelaku pembunuhan itu.

Mereka beralasan dengan hadis yang diriwayatkan oleh Bukhari dan Muslim (muttafaq alaih):

وَفِي رِوَايَةٍ مُّتَّفَقٍ عَلَيْهِ، فَقَالَ لَهُمْ: تَأْتُونَ بِالْبَيِّنَةِ عَلَى مَنْ قَتَلْتَهُ، قَالُوا: مَا لَنَا مِنْ بَيِّنَةٍ، قَالَ: فَيُخْلَفُونَ، قَالُوا: لَا نَرْضَى بِأَيْمَانِ الْيَهُودِ، فَكَرِهَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ أَنْ يُبْطَلَ دَمُهُ فَوَدَّاهُ بِمِائَةِ مِنْ أَهْلِ الصَّدَقَةِ.

Artinya:

Dan di dalam riwayat muttafaq alaih: Maka Nabi berkata kepada mereka (Muhaisah dan Huwaisah): “Kamu sekalian harus mendatangkan saksi atas orang yang membunuhnya. “Mereka berkata: “Kami tidak memiliki saksi. “Nabi berkata: “Kalau begitu mereka (penduduk setempat) harus bersumpah. “Mereka berkata: “Kami tidak suka dengan sumpahnya orang Yahudi. “Maka

Nabi tidak mau membatalkan kasus pembunuhan tersebut, dan akhirnya Nabi membayar diat sebanyak 100 ekor unta yang diambil dari unta zakat.⁷⁵

Apabila mereka (penduduk setempat) bersedia bersumpah, maka diputuskan mereka harus membayar diat kalau pembunuhnya sengaja, dan apabila pembunuhnya tidak sengaja (*al-khat ϕ '*), maka diat dibebankan kepada keluarga penduduk setempat. Apabila mereka tidak bersedia (enggan) bersumpah, maka mereka ditahan (dipenjara) sampai mereka bersedia bersumpah.⁷⁶

2) Menurut Malikiyah, Syafi'iyah, dan Hanabilah serta Dawud al-Zahiri, *qasamah* pertama kali diberikan kepada keluarga korban. Mereka bersumpah lima puluh kali atau lima puluh orang yang menyatakan bahwa mereka (terdakwa) telah membunuh korban. *Lafaz* sumpah bisa dengan:

وَاللّٰهِ الَّذِي لَا إِلَهَ إِلَّا هُوَ عَالِمُ خَائِنَةِ الْأَعْيُنِ وَمَا تُخْفِي الصُّدُورُ.

Artinya:

Demi Allah, yang tidak ada Tuhan kecuali Dia, yang mengetahui pandangan mata yang khianat dan apa yang disembunyikan oleh hati.

Sumpah disyaratkan harus mantap dan pasti yang menyatakan bahwa tersangka melakukan pembunuhan itu sendiri, atau bersama-sama dengan orang lain, ia melakukannya dengan sengaja atau karena kesalahan (tidak sengaja).

Pendapat jumhur ini didasarkan kepada hadis Sahl ibn Abi Hasmah, yang di dalamnya disebutkan:

قَالَ: أَتَخْلِفُونَ وَتَسْتَحِقُّونَ قَاتِلَكُمْ أَوْصَابِكُمْ...

⁷⁵*Ibid.*, h. 404. Lihat juga, Al-Syaukani, VII, *op. cit.*, h. 184.

⁷⁶Wahbah Zuhaili, *op. cit.* h. 404-405.

Artinya:

Nabi berkata: “Apakah kalian bersedia bersumpah dan kalian berhak atas orang yang membunuh teman kalian ...”⁷⁷

Hadis ini menjelaskan bahwa kesempatan pertama untuk melakukan *qasamah* (bersumpah) diberikan kepada keluarga korban, bukan terdakwa.

Apabila para penuntut (keluarga korban) tidak bersedia bersumpah, maka terdakwa dikenai kesempatan untuk bersumpah sebanyak lima puluh kali sumpah. Kalau ia (tersangka) bersedia bersumpah, maka ia dibebaskan dari tuduhan pembunuhan. Syarat-syarat untuk sumpahnya tersangka ini sama dengan syarat-syarat sumpahnya penuntut, yaitu sumpah harus mantap dan pasti bahwa ia tidak melakukan pembunuhan. Misalnya, dalam sumpahnya ia mengatakan:

وَاللّٰهُ مَا قَتَلْتُهُ وَلَا شَارَكْتُ فِي قَتْلِهِ وَلَا فَعَلْتُ سَبِيًّا مَاتَ مِنْهُ وَلَا كَانَ سَبَبًا فِي مَوْتِهِ وَلَا مُعِينًا عَلَى مَوْتِهِ.

Artinya:

Demi Allah, saya tidak membunuhnya, dan saya tidak turut serta dalam membunuhnya, juga tidak melakukan perbuatan yang menjadi sebab kematiannya, serta tidak menjadi sebab, dan tidak menjadi pembantu atas kematiannya.

Apabila para penuntut tidak bersedia bersumpah dan mereka tidak menerima sumpahnya terdakwa, maka para tersangka dibebaskan dari hukuman, dan diat dibayar oleh negara dari Baitul Mal menurut pendapat Imam Ahmad. Akan tetapi, ulama yang lain berpendapat dalam hal ini tidak ada diat.⁷⁸

⁷⁷Al-Syaukani, VII, *op. cit.*, h. 184.

⁷⁸Ibnu Qudamah, VII, *op. cit.*, h. 78.

Apabila para terdakwa menolak untuk bersumpah, maka menurut satu pendapat di dalam Mazhab Hambali, mereka harus ditahan, tetapi menurut pendapat lain tidak. Menurut Imam Malik, mereka (terdakwa) harus ditahan selama satu tahun. Apabila mereka tidak berdedia bersumpah juga, maka mereka dibebaskan. Sedangkan Imam Syafi'i, apabila terdakwa menolak untuk bersumpah, maka sumpah dikembalikan kepada para penuntut. Apabila mereka (penuntut) tidak bersedia bersumpah juga, maka terdakwa dibebaskan dari segala tuntutan. Akan tetapi apabila mereka (penuntut) bersedia bersumpah, maka hukuman diterapkan kepada terdakwa.⁷⁹

Di atas telah dikemukakan bahwa sumpah dalam *qasamah* dilakukan oleh lima puluh orang. Menurut Imam Syafi'i, mereka (kelima puluh orang tersebut) terdiri atas semua ahli waris, baik laki-laki maupun perempuan, termasuk istri dan anak perempuan. Di dalam Mazhab Hambali ada dua pendapat. *Pertama*, sumpah dilakukan ahli waris laki-laki saja, baik *zawil furud* maupun '*asibah*. Sumpah yang lima puluh itu dibagi sesuai dengan jumlah (banyaknya) ahli waris, tetapi tanpa pecahan. Kalau jumlah ahli warisnya sepuluh orang, maka masing-masing ahli waris harus bersumpah sebanyak lima kali. *Kedua*, sumpah dilakukan oleh ahli waris '*asibah* saja. Pendapat ini juga merupakan pendapat Imam Malik. Hanya saja Imam Malik membedakan antara pembunuhan karena kesalahan dan pembunuhan sengaja. Dalam pembunuhan karena kesalahan, sumpah dilakukan oleh semua ahli waris korban, baik *zawil furud* maupun '*asibah*. Sedangkan dalam pembunuhan sengaja, sumpah hanya dilakukan oleh '*asibah* saja.

⁷⁹Abi Ishak al-Sirazi, II, *op. cit.* h. 446. Lihat juga, Abd Qadir Audah, II, *op. cit.*, h. 333.

Menurut Imam Abu Hanifah, *qasamah* hanya dilakukan oleh laki-laki saja. Anak kecil dan orang gila tidak dibebani kewajiban melakukan *qasamah*, meskipun korban ditemukan di atas tanah miliknya. Dalam hal ini *qasamah* dibebankan kepada keluarganya ('*aqilah*). Demikian juga perempuan tidak dibebani kewajiban *qasamah*, kecuali apabila korban ditemukan di rumahnya, dan tidak ada orang lain di dalamnya selain dia.⁸⁰

Sebagai akibat hukum dilaksanakannya *qasamah* adalah diwajibkannya diat, apabila pembunuhannya karena kekeliruan atau menyerupai sengaja. Ketentuan ini disepakati oleh para ulama. Apabila pembunuhannya sengaja, maka hukuman yang harus dijatuhkan diperselisihkan oleh para fukaha. Menurut Imam Malik, dan *qaub qadim* dari mazhab Syafi'i, serta Imam Ahmad, hukuman yang dijatuhkan adalah hukuman diat, baik pembunuhannya sengaja maupun tidak sengaja.⁸¹

Oleh karena itu, pembuktian dengan *qasamah* merupakan suatu terobosan untuk menyelesaikan kasus pembunuhan yang tidak terdapat alat-alat bukti yang lazim, seperti saksi atau pengakuan. Karenanya hukuman yang tertinggi cukup dengan diat bukan *qisas*.

4. *Qarinah*

Pengertian *qarinah* menurut Wahbah Zuhaili adalah sebagai berikut:

الْقَرِينَةُ هِيَ كُلُّ أَمَارَةٍ ظَاهِرَةٍ تَقَارَنُ شَيْئًا خَفِيًّا، فَتَدُلُّ عَلَيْهِ.

Artinya:

⁸⁰ Al-Kasani, VII, *op. cit.* h. 434-435. Lihat juga, Abd. Qadir Audah, II, *op. cit.*, h. 334-336.

⁸¹ *Ibid.*, h. 336-337.

“*Qarīnah* adalah setiap tanda (petunjuk) yang jelas menyertai sesuatu yang samar, sehingga tanda tersebut menunjukkan kepadanya.”⁸²

Dari definisi tersebut dapat dipahami bahwa untuk terwujudnya suatu *qarīnah* harus dipenuhi dua hal, yaitu:

1. Terdapat suatu keadaan yang jelas dan diketahui yang layak untuk dijadikan dasar dan pegangan;
2. Terdapat hubungan yang menunjukkan adanya keterkaitan antara keadaan yang jelas (*ẓāhir*) dan yang tidak jelas atau samar (*khafī*).

Dalam *qarīnah qisṣ*, *qarīnah* hanya digunakan dalam *qasamah*, dalam rangka *ikhtiat* (kehati-hatian) berguna menyelesaikan kasus pembunuhan, dengan berpegang kepada adanya korban ditempat tersangka menurut Hanafiah, atau dengan berpegang kepada adanya *laut* (petunjuk) menurut jumhur ulama. Salah satu contoh *laut* yang kemudian menjadi petunjuk (*qarīnah*) adanya terdapatnya tersangka di dekat kepala korban, dan tangannya memegang pisau yang terhunus, serta badannya berlumuran darah. Adanya tersangka di dekat jasad korban dengan pisau terhunus dan badan serta pakaian yang berlumuran darah merupakan petunjuk (*qarīnah*) bahwa dialah orang ayang membunuh korban. Demikian pula ditemukannya korban di tempat (wilayah) tersangka merupakan *qarīnah* (petunjuk) bahwa pembunuhan dilakukan oleh penduduk wilayah tersebut.

Diperselisihkannya *qarīnah* sebagai alat bukti, sebabnya adalah dalam banyak hal *qarīnah* ini bukan petunjuk yang pasti melainkan masih meragukan, karena itu masih banyak kemungkinan-kemungkinan terjadi. Dalam contoh kasus kehamilan seorang perempuan yang tidak bersuami sebagai *qarīnah* (pertanda) bahwa ia

⁸²*Ibid.*

melakukan zina, belum bisa diterima sebagai petunjuk yang pasti karena masih ada beberapa kemungkinan lain, misalnya ia (perempuan) diperkosa. Oleh karena itu, jumhur fukaha membatasi penggunaan *qarinah* ini dalam kasus-kasus yang adanya nashnya, seperti *qasamah*. Sedangkan para fukaha yang berpendapat bahwa *qasamah* merupakan alat bukti, seperti Ibn al-Qayyim⁸³ memberikan argumentasi, bahwa apabila *qarinah* tidak digunakan akan banyak sekali hak-hak yang hilang dan tercecceh dan ini merupakan suatu kezaliman.

Dari keempat alat bukti tersebut, untuk dapat melacak terhadap tindak pidana *cyber crime*, maka alat bukti yang keempat lebih banyak berperan. Mengapa? Karena alat bukti yang keempat menjadi pintu masuk untuk mengejar kebenaran terhadap tindak pidana *cyber crime*.

Karakteristik perbuatan pidana ini meninggalkan jejak dalam setiap peristiwa tindak pidana. Oleh karena itu *qarinah* (petunjuk) menjadi pintu masuk awal sebelum alat-alat bukti lain berperan.⁸⁴ Tindak pidana *cyber crime* pada umumnya terjadi di ruang tertutup dan tidak diketahui oleh banyak orang. Sehingga alat bukti saksi dan pengakuan secara otomatis sulit untuk diterapkan. Akan tetapi sulit juga untuk menghindari bekas yang ditinggalkan, karena menjadi bukti yang dapat dijadikan sebagai alat bukti petunjuk (*qarinah*).

E. Sanksi Pidana Cyber Crime dalam Hukum Pidana Islam

1. Penipuan

⁸³ Ahmad Wardi Muslich, *op. cit.*, h. 245.

⁸⁴ Alat bukti petunjuk (*qarinah*) tidak serta merta selalu ditempatkan paling awal, akan tetapi melihat kasus tersebut secara kondisional.

Sanksi pidana penipuan sebagaimana penjelasan tersebut di atas, bahwa kejahatan penipuan dilihat dari ruh syariat, menipu adalah membohongi. Berlaku dusta merupakan ciri munafik. Secara tegas dinyatakan dalam hadis nabi sebagai berikut:

عَنْ أَبِي هُرَيْرَةَ رَضِيَ اللَّهُ عَنْهُ: عَنِ النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ قَالَ: (آيَةُ الْمُنَافِقِ ثَلَاثٌ: إِذَا حَدَّثَ كَذَبَ، وَإِذَا وَعَدَ أَخْلَفَ، وَإِذَا أُؤْتِمِرَ بِهِ خَانَ)⁸⁵

Artinya:

Diriwayatkan dari Abu Hurairah ra.: Nabi Muhammad saw. pernah bersabda, “Ada tiga tanda/ciri orang munafik, yaitu: apabila ia berkata ia dusta, apabila ia berjanji ia selalu mengingkari, dan apabila ia diberi amanat, maka ia berkhianat.”

Sifat pembual, pendusta, pembohong dan penipu adalah karakter yang melekat bagi orang munafik. Munafik seperti dinyatakan dalam firman Allah swt. Q.S. al-Nisa'/4: 145 sebagai berikut:

إِنَّ الْمُنَافِقِينَ فِي الدَّرَكِ الْأَسْفَلِ مِنَ النَّارِ وَلَنْ يَجِدَ لَهُمْ نَصِيرًا

Terjemahannya:

Sesungguhnya orang-orang munafik itu (ditempatkan) pada tingkatan yang paling bawah dari neraka. Dan kamu sekali-kali tidak akan mendapat seorang penolong pun bagi mereka.⁸⁶

Ayat tersebut memberikan penilaian kepada orang munafik lebih membahayakan dari pada orang kafir. Jika merampas atau merampok harta hukumannya

⁸⁵Abu al-Husain Muslim ibn al-Hajjaj al-Qusyairi al-Naisaburi, *Sahih Muslim*, Juz IV (Beirut: Dar al-Fikr, 1992 M/1412 H), h.

⁸⁶Departemen Agama RI., *op. cit.*, h. 101.

seperti hukuman orang kafir, yaitu hukuman mati, maka hukuman terhadap orang munafik minimal sama dengan hukuman yang ditentukan terhadap perampok.

Berdasarkan hal tersebut, apabila pelaku tindak pidana penipuan disamakan dengan perbuatan perampok, maka sanksi hukumannya adalah dibunuh yang kemudian disalib, atau dipotong tangan dan kakinya, atau dibuang. Hal ini dilakukan atas dasar besar kecilnya efek yang ditimbulkan dari tindakan tersebut. Apabila dilihat dari sudut pandang *cyber crime*, maka hukuman pokok pada tindak pidana tersebut bisa berupa takzir, karena hakim memiliki otoritas terhadapnya.

2. Kesusilaan

Tindak pidana kesusilaan merupakan bagian dari tindak pidana takzir, yakni termasuk dalam perbuatan-perbuatan yang tidak termasuk dalam kategori *hadd* dan *qisas*.⁸⁷ Penetapan kategori tindak pidananya diserahkan kepada penguasa negara untuk mengaturnya, demikian juga dengan sanksi pidananya. Tindak pidana takzir adalah keseluruhan tindak pidana yang terdapat dalam nas Alquran dan hadis, tetapi tidak ditetapkan sanksi pidananya. Karena tindak pidana kesusilaan muncul di dunia *cyber*, maka tindak pidana ini juga ditetapkan oleh penguasa, karena modus oprandinya yang dinilai baru.⁸⁷ Kewenangan diberikan kepada para legislator untuk merumuskannya.

3. Perjudian

⁸⁷Kasus zina/video mesum dalam konteks Undang-Undang ITE di tempatkan pada pembuktian rekaman yang dijadikan sebagai barang bukti. Untuk itu, rekaman video porno/mesum dapat diuji kebenarannya melalui seorang ahli di bidang IT di laboratorium forensik komunikasi/telematika.

Sebagaimana telah dijelaskan sebelumnya, bahwa apabila dilihat dari aspek hukum Islam, larangan tentang perjudian dan undian dirangkaikan dengan khamar. Dengan dasar itu perjudian dan undian sanksi hukumnya disejajarkan dengan tindak pidana khamar. Hal ini di dasarkan atas firman Allah swt. Swt., Q.S. al-Maidah/5: 90 sebagai berikut:

يَا أَيُّهَا الَّذِينَ آمَنُوا إِنَّمَا الْخَمْرُ وَالْمَيْسِرُ وَالْأَنْصَابُ وَالْأَزْلَامُ رِجْسٌ مِّنْ عَمَلِ الشَّيْطَانِ فَاجْتَنِبُوهُ لَعَلَّكُمْ تُفْلِحُونَ

Terjemahnya:

Wahai orang-orang yang beriman, sesungguhnya (meminum) khamar, berjudi (berkurban untuk) berhala, mengundi nasib dengan panah, adalah perbuatan keji termasuk perbuatan setan. Maka jauhilah perbuatan-perbuatan itu agar kamu mendapat keberuntungan.⁸⁸

Mencermati ayat tersebut, bahwa kedua tindak pidana (perjudian dan khamar) dinilai sebagai suatu perbuatan keji dan biadab. Oleh karena itu dalam ayat tersebut juga menyejajarkan atas hukuman terhadap kedua tindak pidana tersebut.

Sanksi pidana terhadap peminum khamar telah disepakati oleh para ulama, yaitu berupa *had*. Hal ini juga berlaku pada pelaku tindak pidana perjudian, yakni hukuman *had*. Berkaitan dengan bentuk hukumannya para ulama berbeda pendapat, sebagian mengatakan hukumannya akan dijilid sebanyak 80 kali jilid, seperti dikatakan oleh Imam Malik dan Abu Hanifah. Sebagian lagi mengatakan 40 kali jilidan seperti yang dipahami oleh Imam Syafi'i. meskipun demikian pendapat terakhir ini membolehkan (kalau dikehendaki penguasa/ulil amri) penambahan 40

⁸⁸Departemen Agama RI., *loc. cit.*

kali lagi, sebagai hukuman takzir. Pelaksanaan hukuman jilid bagi pelaku *jarimah* ini sama seperti hukuman jilid pada jarimah lain yang mengharuskan hukuman jilid.⁸⁹

Hukuman jilid (cambuk) juga diadopsi oleh Negara Republik Indonesia, di mana negara Indonesia yang mengkhususkan daerah tertentu dengan menggunakan aturan otonomi khusus untuk menerapkan hukuman cambuk atau jilid sebagai hukuman yang dinilai cukup efektif. Hal ini dilakukan semata-mata untuk mewujudkan rasa keadilan dan kemunusiaan yang sekaligus menjadi ciri dari pemidanaan dalam Islam.

4. Pemerasan/Pengancaman

Pemerasan yang disertai pengancaman pada dasarnya mengambil harta atau pemindahan hak kepemilikan harta benda milik orang lain dalam penguasaannya tanpa transaksi yang sah disertai dengan pemaksaan. Sehingga modus yang dilakukan terhadap kejahatan ini bermacam-macam. Tetapi substansinya ingin memiliki harta dengan cara yang tidak benar. Tindak pidana ini dapat pula dikiaskan dengan penodongan atau perampokan dengan illat mengambil harta atau pemindahan hak kepemilikan harta benda milik orang lain dalam penguasaannya tanpa transaksi yang sah disertai dengan pemaksaan. Penodongan lebih lazim dipakai terhadap tindak pidana yang dilakukan di luar rumah, sedangkan perampokan dilakukan di dalam rumah atau kantor. Sehingga sanksi hukumnya dapat dijatuhkan berdasarkan ketentuan pokok dalam pencurian dan perampokan, yaitu dibunuh yang kemudian disalib, atau pidana amputasi tangan dan kaki yang merupakan sebagai sanksi pidana pokok tindak pidana takzir.

⁸⁹Rahmat Hakim, *op. cit.*, h. 101.

Akan tetapi, dengan melihat kenyataan terhadap perbuatan pidana yang dilakukannya sanksi hukumnya dapat berupa hukuman yang lebih ringan, seperti misalnya pidana cambuk, pidana penjara, pidana denda, pidana pengawasan dan lain-lain bahkan bebas dari segala tuntutan hukum. Penjatuhan hukuman tentu setelah melalui proses peradilan (persidangan) dan memenuhi syarat-syaratnya.

5. Pengrusakan

Tindak pidana pengrusakan dalam hukum pidana Islam dikelompokkan dalam tindak pidana atas selain jiwa. Akan tetapi, tindak pidana pengrusakan dalam *cyber crime* tidak menyangkut pengrusakan yang berkaitan anggota badan, melainkan dokumen elektronik atau sejenisnya. Untuk pengrusakan dokumen elektronik disamakan dengan hirabah dengan illat mengganggu keamanan, maka hukumannya potong tangan dan kaki secara bersilang karena hirabah yang disamakan dalam kasus ini adalah mengambil harta secara terang-terangan tanpa membunuh pemiliknya.

Merujuk dari jenis tindak pidana pengrusakan dalam tindak pidana atas selain jiwa, maka hukumannya ditentukan atas berat ringannya akibat yang menimpa sasaran atau obyek tindak pidana, bukan kepada niat pelaku. Hal serupa juga berlaku atas pengrusakan terhadap barang atau program dalam komputer.

Sehingga untuk hukuman atau sanksi terhadap pelaku kejahatan dalam dunia *cyber*, harus diketahui secara pasti dari dampak atau efek dari kejahatan tersebut.

6. Pencurian

Pencurian dalam bentuk dokumen elektronik dapat disamakan dengan *sariqah* (pencurian) dengan illat mengambil barang orang lain secara diam-diam dari tempat penyimpanan. Pencurian dalam syari'at Islam ada 2 (dua) macam, yaitu sebagai berikut:

- a. Pencurian yang hukumnya *hadd*.
- b. Pencurian yang hukumannya takzir.

Pencurian yang hukumannya *hadd* terbagi atas dua bagian, yaitu:

- 1) Pencurian ringan,
- 2) Pencurian berat.

Pencurian ringan menurut rumusan yang dikemukakan oleh Abdul Qadir Audah adalah sebagai berikut:

فَأَمَّا السَّرْقَةُ الصُّغْرَىٰ فَهِيَ أَخَذَ مَالِ الْغَيْرِ خُفْيَةً أَيْ عَلَىٰ سَبِيلِ الْإِسْتِخْفَاءِ.

Artinya:

Pencurian ringan adalah mengambil harta milik orang lain dengan cara diam-diam, yaitu dengan jalan sembunyi-sembunyi.⁹⁰

Sedangkan pengertian pencurian berat adalah sebagai berikut:

أَمَّا السَّرْقَةُ الْكُبْرَىٰ فَهِيَ أَخَذَ مَالِ الْغَيْرِ عَلَىٰ سَبِيلِ الْمُغَالَبَةِ

Artinya:

Adapun pengertian pencurian berat adalah mengambil harta milik orang lain dengan cara kekerasan.⁹¹

Perbedaan antara pencurian ringan dengan berat adalah bahwa dalam pencurian ringan, pengambilan harta itu dilakukan tanpa sepengetahuan pemilik dan tanpa persetujuannya. Sedangkan dalam pencurian berat, pengambilan tersebut dilakukan dengan sepengetahuan pemilik harta tetapi tanpa kerelaannya, di samping

⁹⁰ Abdul Qadir Audah, Jil. II, *op. cit.*, h. 514.

⁹¹ *Ibid.*

terdapat unsur kekerasan. Dalam istilah lain, pencurian berat itu disebut *jarimah hirabah* atau perampokan. Perampokan dimasukkan dalam kelompok pencurian, karena dalam perampokan terdapat segi persamaan dengan pencurian, yaitu sekalipun dikaitkan dengan pemilik barang, perampokan itu dilakukan dengan terang-terangan, namun jika dikaitkan dengan pihak penguasa atau petugas keamanan, perampokan tersebut dilakukan dengan sembunyi-sembunyi.

Pencurian yang hukumannya takzir juga dibagi menjadi dua bagian, yaitu sebagai berikut:

1. Semua pencurian yang dikenai hukuman *hadd*, tetapi syarat-syaratnya tidak terpenuhi, atau *syubhat*. Contohnya: seperti pengambilan harta milik anak oleh ayahnya,
2. Pengambilan harta milik orang lain dengan sepengetahuan pemilik tanpa kerelaannya dan tanpa kekerasan. Contohnya seperti menjambret kalung dari leher seorang wanita, lalu penjambret itu melarikan diri dan pemilik barang tersebut melihatnya sambil berteriak meminta bantuan.

Menurut Ahmad Wardi Muslich,⁹² definisi yang dikemukakan oleh Abdul Qadir Audah belum sempurna. Menurutnya definisi yang sempurna dikemukakan oleh Muhammad Abu Syahbah, sebagai berikut:

السَّرْقَةُ شَرْعًا، هِيَ أَخْذُ الْمُكَلَّفِ -أَيُّ الْبَالِغِ الْعَاقِلِ- مَالٍ الْغَيْرِ خَفِيَّةً إِذَا بَلَغَ نَصَابًا، مِنْ خِرَزٍ
مِنْ غَيْرٍ أَنْ يَكُونَ لَهُ شُبْهَةٌ فِي هَذَا الْمَالِ الْمَأْخُوذِ.

Artinya:

Pencurian menurut syarak adalah pengambilan oleh seorang mukalaf (yang balig dan berakal) terhadap harta milik orang lain dengan diam-diam, apabila

⁹²Ahmad Wardi Muslich, *Hukum Pidana Islam* (Cet. I; Jakarta: Sinar Grafika, 2005), h. 82.

barang tersebut mencapai nisab (batas minimal), dari tempat simpanannya, tanpa ada *syubhat* dalam barang yang diambil tersebut.⁹³

Berdasarkan rumusan tersebut, maka dapat diketahui bahwa unsur-unsur dalam pencurian itu ada empat macam, yaitu sebagai berikut:

1. Perbuatan mengambil dilakukan secara diam-diam/sembunyi;
2. Barang yang diambil itu berupa harta sampai nisab yang disepakati;
3. Harta tersebut milik orang lain;
4. Adanya keinginan untuk memiliki dengan cara melawan hukum.

Apabila salah satu unsur tidak terpenuhi, maka perbuatan itu tidak dapat disebut sebagai pencuri, melainkan dengan penyebutan yang lainnya. Berdasarkan hal tersebut, maka pelaku tindak pidana pencurian apabila dapat dibuktikan dapat dihukum dengan 2 (dua) macam hukuman, yaitu sebagai berikut:

1. Penggantian Kerugian

Menurut Imam Abu Hanifah dan murid-muridnya, penggantian kerugian dapat dikenakan terhadap pencuri apabila ia tidak dikenai hukuman potong tangan. Akan tetapi, apabila hukuman potong tangan dilaksanakan, maka pencuri tidak dikenai penggantian kerugian. Dengan demikian menurut mereka, hukuman potong tangan dan penggantian kerugian tidak dapat dilaksanakan sekaligus bersama-sama. Alasannya adalah bahwa Alquran hanya menyebutkan hukuman potongan tangan untuk tindak pidana pencurian, sebagaimana tercantum dalam Surah Al-Maidah ayat 38, dan tidak menyebut-nyebut penggantian kerugian.⁹⁴

⁹³Muhammad Abu Syahbah, *Al-Hudud fi Al-Islam, al-Hai'ah Al-'Ammah li Syuuni* (Kairo: Al-Mathabi' Al-Amiriyah, 1974), h. 215.

⁹⁴Al-Kasani, VII, h. 125. Lihat juga, Sayid Sabiq, *op. cit.*, h. 426.

Menurut Imam Syafi'i dan Imam Ahmad, hukuman potong tangan dan hukuman kerugian penggantian dapat dilaksanakan secara bersama-sama. Alasannya adalah bahwa dalam pencurian terdapat dua hak yang disinggung, pertama hak Allah dan kedua hak manusia. Hukuman potong tangan dijatuhkan sebagai imbalan dari hak Allah, sedangkan penggantian kerugian dikenakan sebagai imbalan dari hak manusia.⁹⁵

Menurut Imam Malik dan murid-muridnya, apabila barang yang dicuri sudah tidak ada dan pencuri adalah orang yang mampu, maka ia diwajibkan untuk mengganti kerugian sesuai dengan nilai barang yang dicuri, di samping dikenai hukuman potong tangan. Akan tetapi, apabila ia tidak mampu, maka ia hanya dijatuhi hukuman potong tangan dan tidak dikenai penggantian kerugian.⁹⁶

2. Hukuman Potong Tangan

Hukuman potong tangan merupakan hukuman pokok untuk tindak pidana pencurian. Ketentuan ini didasarkan kepada firman Allah dalam Q.S. Al-Maidah/5: 38, sebagai berikut:

وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالًا مِّنَ اللَّهِ ۚ وَاللَّهُ عَزِيزٌ حَكِيمٌ. فَمَن تَابَ مِن بَعْدِ ظُلْمِهِ وَأَصْلَحَ فَإِنَّ اللَّهَ يَتُوبُ عَلَيْهِ ۚ إِنَّ اللَّهَ غَفُورٌ رَّحِيمٌ.

Terjemahannya:

Laki-laki yang mencuri dan perempuan yang mencuri, potonglah tangan keduanya, sebagai pembalasan bagi apa yang mereka kerjakan dan sebagai siksaan dari Allah. Dan Allah Maha Perkasa lagi Maha bijaksana.⁹⁷

⁹⁵ Abdul Qadir Audah, II, *op. cit.*, h. 620.

⁹⁶ Sayid Sabiq, *loc. cit.*

⁹⁷ Departemen Agama RI, *op. cit.*, h. .

Hukuman potong tangan merupakan hak Allah yang tidak dapat digugurkan, baik oleh korban maupun oleh ulil amri, kecuali menurut Syi'ah Zaidiyah. Menurut mereka, hukuman potong tangan dapat gugur apabila dimaafkan oleh korban (pemilik barang).⁹⁸

Hukuman potong tangan dikenakan terhadap pencuri yang pertama, dengan cara memotong tangan kanan pencuri dari pergelangan tangannya. Apabila ia mencuri untuk kedua kalinya, maka ia dikenai hukuman potong kaki kirinya. Apabila ia mencuri lagi untuk ketiga kalinya, maka ulama berbeda pendapat. Menurut Imam Abu Hanifah, pencuri tersebut dikenai hukuman takzir dan dipenjarakan. Sedangkan menurut Imam Malik, Imam Syafi'i dan Imam Ahmad, pencuri tersebut dikenai hukuman potong tangan kirinya. Apabila ia masih mencuri untuk kelima kalinya, maka ia dikenai hukuman takzir dan dipenjara seumur hidup (sampai mati) atau sampai ia bertobat.⁹⁹

Pendapat jumhur tersebut didasarkan kepada hadis Nabi saw. Yang diriwayatkan oleh al-Daruquthni dari Abu Hurairah, Nabi saw. Bersabda dalam kaitan dengan hukuman bagi pencuri:

ان سَرَقَ فَاقْطَعُوْا يَدَهُ ثُمَّ اِنْ سَرَقَ فَاقْطَعُوْا رِجْلَهُ، ثُمَّ اِنْ سَرَقَ فَاقْطَعُوْا رِجْلَهُ.
 ALAUDDIN
 M A K A S S A R

Artinya:

Jika ia mencuri maka potonglah tangannya (yang kanan), jika ia mencuri lagi maka potonglah kakinya (yang kiri), jika ia mencuri lagi potonglah tangannya

⁹⁸*Ibid.*, h. 425.

⁹⁹Abdul Qadir Audah, II, *op. cit.*, h. 623.

(yang kiri), kemudia jika ia mencuri lagi maka potonglah kakinya (yang kanan).¹⁰⁰

Adapun batas pemotongan menurut ulama yang empat, yaitu Imam Malik, Imam Abu Hanifah, Imam Syafi'i dan Imam Ahmad adalah dari pergelangan tangan. Sedangkan menurut Khawarij pemotongan dari pundak. Alasan jumhur ulama adalah karena pengertian adalah karena pengertian minimal dari tangan itu adalah telapak tangan dan jari. Alasan Khawarij adalah karena pengertian tangan itu mencakup keseluruhan dari sejak ujung jari sampai batas pundak.¹⁰¹

Berdasarkan dari uraian di atas, maka keseluruhan sanksi pidana yang telah ditetapkan masing-masing tindak pidana terdapat sanksi pidan secara maksimal dan sanksi pidana ringan. Karena sanksi pidana ditetapkan berdasarkan tingkat berat dan ringannya kejahatan dan tingkat efek yang terjadi pada korban, maka sanksinya pun beraneka ragam.

Mengingat Indonesia merupak negara berasaskan Pancasila yang mengacu pada hukum positif dan memberlakukan Undang-Undang ITE sebagai undang-undang yang mengatur *cyber crime* bukan hukum pidana Islam, maka sanksi yang telah ditetapkan secara maksimal dalam hukum pidana Islam dapat diturunkan menjadi sanksi jarimah takzir, yakni sanksi hukumannya diserahkan kepada penguasa atau hakim untuk menyelesaikan perkara-perkara yang berkaitan dengan *cyber crime* karena penguasa atau hakim memiliki otoritas terhadap penetapan sanksinya, yaitu penjara dan denda.

¹⁰⁰Muhammad Ibn Isma'il Al-Kahlani, IV, *op. cit.*, h. 27.

¹⁰¹Abdul Qadir Audah, II, *op. cit.*, h. 628.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan uraian pada bab-bab sebelumnya dapat dirumuskan beberapa kesimpulan sebagai jawaban terhadap permasalahan dalam penelitian ini, antara lain:

1. *Cyber crime* dalam Undang-Undang ITE pada hakikatnya adalah kejahatan yang dilakukan oleh pelaku dengan menggunakan sarana teknologi informasi (internet) dan sejenisnya. Perbuatan *cyber crime* telah diatur secara spesifik melalui Undang-Undang ITE tercantum dalam Bab 7 untuk “Perbuatan yang Dilarang” yakni pada Pasal 27-37 dan dalam Bab 11 untuk “Ketentuan Pidana” pada Pasal 45-52.

2. Hukum pidana Islam melihat *cyber crime* sebagai suatu kejahatan nyata, tetapi maya yang mengalami modernisasi pada aspek modus operandi dan memiliki kesamaan terhadap hukum pidana Islam pada aspek substansi. Karena kejahatan yang terjadi pada dunia *cyber* merupakan pengembangan dari bentuk kejahatan yang cikal bakalnya telah ada pada zaman dahulu kala dan berkembang secara pesat melalui perkembangan informasi dan teknologi. Kejahatan yang terlihat pada saat ini merupakan bentuk modernisasi yang mengiringi perkembangan *cyber cpace* (dunia maya/internet). *Cyber crime* dilihat dari sudut pandang hukum pidana Islam yang menjadi landasan pokok adalah terhadap aspek yuridis, adalah teori *maqasid al-syari'ah* meletakkan prinsip-prinsip yang menjadi pertimbangan pokok dari tujuan hukum, yaitu terwujudnya kemaslahatan manusia baik di dunia maupun di akhirat, yaitu terwujud dan terpeliharanya *al-masā'il al-khamsah* atau lima kebutuhan pokok dalam kehidupan manusia yang mencakup pemeliharaan agama (*hifz al-din*), jiwa

(*hifz}al-nafs*), keturunan atau kehormatan (*hifz}al-nasl*), harta (*hifz}al-mal*) dan akal (*hifz} al-'aql*). Sehingga kenyataan dalam praktik-praktik *cyber crime* dinilai melanggar lima kebutuhan pokok dalam kehidupan manusia tersebut.

3. Sanksi pidana dalam ketentuan Undang-Undang ITE, bahwa para pelaku tindak pidana *cyber crime* dipidana dengan ketentuan sebagai berikut: 1) *pencurian*, dipidana 6 (enam) tahun dan denda Rp. 1 milyar, 2) *kesusilaan*, dipidana 6 (enam) tahun dan denda Rp. 1 milyar, 3) *perjudian*, dipidana 6 (enam) tahun dan denda Rp. 1 milyar dan jika dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga. 4) *Pengancaman*, meliputi dua kategori yakni; *pemerasan/pengancaman biasa* dipidana 6 (enam) tahun dan denda Rp. 1 milyar dan jika dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga. Sedangkan untuk *pengancaman disertai kekerasan* dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 2. miliar. 5) *Pengrusakan*, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10 miliar. 6) *Pencurian*, mengakses komputer dan/atau sistem elektronik milik orang lain dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600 juta, mengakses komputer tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700 juta, mengakses dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800 juta. Apabila pencurian itu dilakukan dengan obyek milik pemerintah dan/atau digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga. Selain itu, jika obyeknya milik pemerintah dan/atau badan strategis

termasuk dan tidak terbatas pada lembaga pertahanan, bank central, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing pasal ditambah dua pertiga.

Sedangkan sanksi pidana dalam hukum pidana Islam ditentukan sebagai berikut: 1) *penipuan*, sanksi pidannya dibunuh kemudian disalib, atau dipotong tangan dan kakinya, atau dibuang. 2) *kesusilaan*, sanksi pidananya di serahkan kepada pemerintah (penguasa) atau diserahkan kepada para legislator untuk merumuskannya. 3) *perjudian*, sanksi hukumnya disejajarkan dengan khamar, yakni jilid atau cambuk sebanyak 80 kali cambukan. 4) *pemerasan/pengancaman*, sanksi hukannya amputasi tangan dan kaki, atau pidana cambuk, penjara, pidana denda dan pidana pengawasan. 5) *pengrusakan*, sanksi pidananya tergantung efek atau dampak dari kejahatan tersebut. 6) *pencurian*, sanksi pidananya adalah potong tangan dan penggantian kerugian.

B. Rekomendasi Penelitian

Berdasarkan hasil kesimpulan tersebut, maka rekomendasi penelitian ini adalah sebagai berikut:

1. Perumusan perundang-undangan yang baik adalah perumusan undang-undang yang melihat seluruh aspek kehidupan sebagai landasan yang harus dipertimbangkan, sehingga tidak memunculkan polemik baru di kemudian hari. Realitas yang terjadi banyak perundang-undangan yang disengketakan (*judicial review*) di Mahkamah Konstitusi (MK) yang berakhir ditolaknya perundang-undangan untuk diundangkan, karena bertentangan dengan perundang-undangan yang berlaku sebelumnya atau perundang-undangan yang lebih tinggi dan bahkan

dalam pasal-pasal tersebut dinilai mengandung pasal karet (pasal yang mengandung multi tafsir) yang dapat ditafsirkan oleh siapa saja berdasarkan kehendaknya sendiri.

Oleh karena itu, rumusan perundang-undangan tersebut harus memenuhi unsur-unsur dari sebuah kejahatan atau tindak pidana yang dimaksud, baik unsur subyektif maupun obyektif.

2. Esensi pembuktian dalam hukum acara pidana adalah untuk mencari kebenaran materiil. Dalam konteks ini, kejahatan dalam bentuk apapun dan dimana pun pada dasarnya dapat dibuktikan. Hanya persoalannya adalah apakah perundang-undangan itu mengaturnya? Oleh karena itu, pihak-pihak yang berwenang berkewajiban menggali dan mengkaji terhadap aspek-aspek hukum baik formil dan materiil.

3. Mengacu pada teori pembedaan, bahwa pembedaan tidak hanya sekedar berorientasi pada balas dendam dan efek jera, tetapi juga mempertimbangkan aspek filosofis dan sosiologis. Oleh karena itu, sanksi pidana untuk kejahatan *cyber crime* harus lebih mengarah pada pembinaan dan upaya menertibkan kehidupan masyarakat.

DAFTAR PUSTAKA

- ‘Amir, Abd. Aziz. *Al-Ta’zīfī al-Syari’ah al-Islamiyah*. Cet. IV; [t.t]: Dar al-Fikr al-‘Arabi, 1969.
- Ali, Mohammad Daud. *Hukum Islam: Pengantar Ilmu Hukum dan Tata Hukum Islam di Indonesia*. Jakarta: PT RajaGrafindo Persada, 2007.
- Ali, Zainuddin. *Hukum Islam: Pengantar Ilmu Hukum Islam di Indonesia*. Jakarta: Sinar Grafika, 2008.
- _____. *Hukum Pidana Islam*. Cet. I; Jakarta: Sinar Grafika, 2007.
- Arief, Barda Nawawi. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Cet. II; Jakarta: Kencana, 2008.
- _____. *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*. Cet. I; Bandung: PT Citra Aditya Bakti, 2005.
- _____. *Hukum Islam Pengantar Ilmu Hukum Islam di Indonesia*. Cet. II; Jakarta: Sinar Grafika, 2008.
- Arikunto, Suharsini. *Manajemen Penelitian*. Cet. IV; Jakarta: Rineka Cipta, 1998.
- _____. *Prosedur Penelitian (Suatu Pendekatan Praktik)*. Jakarta: Rineka Cipta, 2002.
- Astuti, Made Shadi. *Pemidanaan Terhadap Anak sebagai Pelaku Tindak Pidana*. Malang: IKIP Malang, [t.th.].
- Audah, Abdul Qadir. *Al-Tasyri’ al-Jina’iy al-Islamiy*. Juz I; Beirut: Dar Al-Kitab Al’arabi, [t.th.].

- Az-Zuhaili, Wahbah. *Nazhariyah al-Dharurah al-Syari'ah Muqaranah Ma'a al-Qanun al-Wadh'i*. Terj. Said Agil Husain al-Munawar dan M. Hadari Hasan, *Konsep Darurat dalam Hukum Islam: Studi Banding dengan Hukum Positif*. Cet. I; Jakarta: Gaya Media Pratama, 1997.
- Bahri, Syamsul. *Metodologi Hukum Islam*. Cet. I: Yogyakarta: Teras, 2008.
- Bakri, Muammar. *Fikih Prioritas: Konstruksi Metodologi Hukum Islam dan Kompilasi Kaidah Prioritas Hukum Islam*. Cet. I; Jakarta: Pustaka Mapan, 2008.
- Bisri, Cik Hasan. *Pilar-pilar Penelitian Hukum Islam dan Pranata Sosial*. Cet. I; Jakarta: PT RajaGrafindo Persada, 2004.
- Chazawi, Adami. *Pelajaran Hukum Pidana (Bagian I)*. Malang: Biro Konsultasi dan Bantuan Hukum Fakultas Hukum Universitas Brawijaya, 2001.
- Departemen Agama RI. *Alquran dan Terjemahnya*. Bandung: PT Syaamil Cipta Media, 2004.
- Dijk, J. J. M. Van, *et all. Actuele Criminologie* diterjemahkan oleh Soemitro. Surakarta: Universitas Sebelas Maret Press, 1996.
- Djazuli, H.A. *Kaidah-Kaidah Fikih: Kaidah-kaidah Hukum Islam dalam Menyelesaikan Masalah-Masalah yang Praktis*. cet I; Jakarta: Prenada Media Group, 2006.
- Echols, John M., dan Hassan Shadily. *Kamus Inggris-Indonesia*. Cet. XXV; Jakarta: Gramedia Pustaka Utama, 2003.
- F.N., Kerlinger. *Foundation and Behavior Research*, Alih Bahasa Simatupang Landung R., *Asas-asas Penelitian Behavior*. Yogyakarta: Gajah Mada University Press, 2006.
- Friedman, M. Lawrence. *Law and Society: An Introduction*. Englewood Cliff: Prentice Inc., 1977.

- Fuad, Mahsun. *Hukum Islam Indonesia dan Nalar Partisipatoris Hingga Emansipatoris*. Cet. I; Yogyakarta: LKiS Yogyakarta, 2005.
- Hakim, Rahmat. *Hukum Pidana Islam (Fikih Jinayah)*. Bandung: CV Pustaka Setia, 2000.
- Hamzah, Jur. Andi. *Hukum Acara Pidana Indonesia*. Cet. II; Jakarta: Sinar Grafika, 2008.
- Haq, Hamka. *Syariat Islam Wacana dan Penerapannya*. Ujung Pandang: Yayasan al-Ahkam, 2001.
- Ikhwansyah, Isis. *Prinsip-prinsip Universal Bagi Kontrak Melalui E-Commerce dan Sistem Hukum Pembuktian Perdata dalam Teknologi Informasi, dalam Cyberlaw: Suatu Pengantar*, Bandung: ELIPS, 2002.
- Institut Komputer Indonesia (IKI). *Pengenalan Komputer (Introduction to computer)*. Jakarta: [t.p.], 1981.
- al-Jauziah, Ibn al-Qayyim. *I'lam al-Muwaqqi'in al-Rabbil 'Alamin*. [t.tp]: Dar al-Fikr, 1877.
- Karjadi, M. dan R. Soesilo. *Kitab Undang-Undang Hukum Acara Pidana Lengkap dengan Penjelasan Resmi dan Komentar seta Peraturan Pemerintah R.I. Nomor 27 Tahun 1983 tentang Pelaksanannya*. Bogor: Politeia, 1997.
- Kartanegara, Satochid. *Hukum Pidana Kumpulan Kuliah*. Buku I; Jakarta: Balai Lektur Mahasiswa, [t.th.].
- al-Kahlani, Muhammad Ibn Ismail. *Subl al-Salam*. Juz VI; Mesir: Maktabah Mushtafa al-Baby al-Halaby, 1960.
- Khallaf, Abdul Wahab. *Kaidah-kaidah Hukum Islam (Ilmu Ushulul Fiqh)*. Cet. VI; Jakarta: PT RajaGrafindo Persada, 1996.

- al-Kasani, 'Ala al-Din. *Kitab Badai' al-Shanai' fi Tartib al-Syara'i*. Beirut: Dar al-Fikr, 1996.
- Lamintang, P.A.F. dan Djisman Samosir. *Delik-Delik Khusus Kejahatan yang Ditujukan Terhadap Hak Milik dan Lain-lain Hak yang Timbul dari Hak Milik*. Bandung: Penerbit Tarsito, 1980.
- Lamintang, P.A.F. *Dasar-Dasar Hukum Pidana Indonesia*. Citra Aditya Bakti, 1997.
- _____. *Hukum dan Telematika: Kerangka Teknologi Informasi Nasional*. Jakarta: Tim Koordinasi Telematika Indonesia, 2001.
- Longman Group. *Longman dictionary of Contemporary English*. Ed. VIII; England: [t.tp], 1998.
- Lubis, Todung Mulya. *Hak Asasi Manusia dan Pembangunan*. Jakarta: YLBHI, 1987.
- Makarim, Edmund. *Kompilasi Hukum Telematika*. Jakarta: PT RajaGrafindo Persada, 2003.
- Manan, H. Abd. *Reformasi Hukum Islam di Indonesia*. Jakarta: PT RajaGrafindo Persada, 2006.
- Mansur, Dikdik M. Arief dan Elisatris Gultom. *Cyber Law: Aspek Hukum Teknologi Informasi*. Cet. I; Bandung: PT Refika Aditama: 2005.
- Mansur, Dikdik M. Arief, dan Arisatris Gultom. *Cyber Law, Aspek Hukum Teknologi Informasi*. Bandung: PT Refika Aditama, 2005.
- Mardalis. *Metode Penelitian Suatu Pendekatan Proposal*. Jakarta: Bumi Aksara Putra, 1993.
- Al-Maqdisi, Abdullah Ibn Qudamah. *Al-Mugni*. [t.tp]: Dar al-Manar, [t.tp].

- Mawardi, Abu al-Hasan. *Al-Ahkam al-Sultaniyyah*. Cet. II; Mesir: Mustafa al-Babi al-Halabi, 1975.
- Mubarok, Jaih. *Sejarah dan Perkembangan Hukum Islam*. Cet. II; Bandung: PT Remaja Rosda Karya, 2000.
- Muslich, Ahmad Wardi. *Hukum Pidana Islam*. Jakarta: Sinar Grafika, 2005.
- Muslich, H. Ahmad Wardi. *Hukum Pidana Islam*. Cet. I; Jakarta: Sinar Grafika Offset, 2005.
- Al-Naisaburi, Abu al-Husain Muslim ibn al-Hajjaj al-Qusyairi. *Sahih Muslim*, Juz IV. Beirut: Dar al-Fikr, 1992 M/1412 H.
- Nitibaskara, Tubagus Ronny Rahman. *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi dan Sosiologi*. Jakarta: Peradaban, 2001.
- Oetomo, Hadi Sutedjo Dharma, Ester Wibowo, Eddy Hartono dan Samuel Prakoso. *Pengantar Teknologi Informasi Internet, Konsep dan Aplikasi*. Ed. I; Yogyakarta: Andi Offset, 2007.
- Pandoyo, S. Toto. *Wawasan Nusantara dan Implementasinya dalam UUD 1945 Serta Pembangunan Nasional*. Cet. II; Jakarta: PT. Rineka Cipta, 1994.
- Panjaitan, Hinca IP, et al. *Membangun Cyber Law Indonesia yang Demokratis*. Jakarta: IMLPC, 2005.
- Purbo, Onno W. "Hadapi Kejahatan Internet, KUHP Perlu Disempurnakan". <http://www.hukum.online> (27 April 2005).
- Raharjo, Agus. *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya Bakti, 2002.
- Ramli, Ahmad M., Pager Gunung dan Indra Apriadi. *Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik*. Jakarta: Departemen Komunikasi dan Informatika RI, 2005.

- Ramli, Ahmad M. *Cyber Law dan Haki dalam Sistem Hukum Indonesia*. Cet. I; Bandung: PT Refika Aditama, 2004.
- Ramulyo, Mohd. Idris. *Asas-asas Hukum Islam Sejarah Timbul dan Berkembangnya Kedudukan Hukum Islam di Indonesia*. Cet. I; Jakarta: Sinar Grafika, 1995.
- Redaksi New Merah Putih. *Undang-Undang ITE (Informasi dan Transaksi Elektronik)*. Cet. I; Yogyakarta: New Merah Putih, 2009.
- Riswandi, Budi Agus. *Hukum Cyber Space*. Cet. I; Yogyakarta: Gitanagari, 2006.
- Rofiq, Ahmad. *Hukum Islam di Indonesia*. Cet. VI; Jakarta: PT RajaGrafindo Persada, 2003.
- Rosyada, Dede. *Hukum Islam dan Pranata Sosial*. Jakarta: Lembaga Studi Islam dan Kemasyarakatan, 1992.
- Sabiq, Sayid. *Fiqh al-Sunnah*. Beirut: Dar Al-Fikr, 1980.
- Sahetapy, J. E. *Kriminologi*. Jakarta: Rajawali, 1998.
- _____, J.E. *Hukum Pidana*. Yogyakarta: Liberty, [t.th.].
- Samin, Sabri. *Pidana Islam dalam Politik Hukum Indonesia Eklektisisme dan Pandangan Non Muslim*. Cet. I; Jakarta: Kholam Publishing, 2008.
- Santoso, Topo dan Eva Achjani Zulfa. *Kriminologi*. Jakarta: PT RajaGrafindo Persada, 2005.
- Sanusi, M. Arsyad. *E-Commerce: Hukum dan Solusiny*. (Bandung: PT. Mizan Grafika Sarana, 2001.
- Sasangka, Hari dan Ahmad Rifai. *KUHP (Kitab Undang-Undang Hukum Pidana) Disertai Yurisprudensi Mahkamah Agung Republik Indonesia*. Bandung: CV. Mandar Maju, 2010.

- Satori, Djam'an dan Aan Komariah. *Metode Penelitian Kualitatif*. Cet. I; Bandung: Alfabeta, 2009.
- Sirry, Mun'im A. *Sejarah Fikih Islam Sebuah Pengantar*. Cet. II; Surabaya: Risalah Gusti: 1996.
- Soekanto, Soerjono. *Pokok-Pokok Sosiologi Hukum*. Rajawali Pers, 1980.
- _____. *Faktor-faktor yang Memengaruhi Penegakan Hukum*. Jakarta: PT RajaGrafindo Persada, 2008.
- Soesilo, R. *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-komentarnya Lengkap Pasal Demi Pasal*. Bogor: Politeia Bogor, 1998.
- Subekti. *Hukum Pembuktian*. Jakarta: Pradnya Paramita, 1983.
- Suharto, R.M. *Hukum Pidana Materiil Unsur-unsur Obyektif Sebagai Dasar Dakwaan*. Jakarta: Sinar Grafika, 1991.
- Sulaiman, Robinton. *Cyber Crime: Perspektif E-Commerce Crime*. Jakarta: Universitas Pelita Harapan, 2002.
- Suparni, Niniek. *Cyber Space: Problematika dan Antisipasi Pengaturannya*. Cet. I; Jakarta: Sinar Grafika, 2009.
- Suratmaputra, Ahmad Munif. *Filsafat Hukum Islam. Al-Ghazali Masalah Mursalah dan Relevansinya dengan pembaharuan Hukum Islam*. Cet. I; Jakarta: Pustaka Firdaus, 2002.
- Sutarman. *Cyber Crime Modus Operandi dan Penanggulangannya*. Cet. I; Yogyakarta: LaksBang PRESSindo, 2007.
- Al-Syabbah, Muhammad Abu. *Al-Hudud fi Al-Islam, al-Hai'ah Al-'Ammah li Syuuni*. Kairo: Al-Mathabi' Al-Amiriyah, 1974.

Al-Syaukani, Imam. *Rekonstruksi Epistemologi Hukum Nasional*. Jakarta: PT RajaGrafindo Persada, 2006.

Al-Syaukani, Muhammad Ibn Ali, *Nail al-Authar*, Juz VII; Beirut, Dar al-Fikr, [t.th.].

Tim Andi Yogyakarta dan Wahana Komputer Semarang. *Kamus Lengkap Dunia Komputer*. Edisi I; Yogyakarta: Andi Yogyakarta dan Wahana Komputer Semarang, 2002.

Tongat. *Dasar-dasar Hukum Pidana Indonesia dalam Perspektif Pembaharuan*. Cet. II; Malang: UMM Press, 2009.

Unais, Ibrahim *et al.* *Al-Mu'jam al-Wasit*, [t.tp]: Dar Ihya' al-Turats, [t.th].

Wahid, Abdul dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Cet. I; Bandung: Refika Aditama, 2005.

Widodo. *Sistem Pidana dalam Cyber Crime: Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime*. Cet. I; Yogyakarta: Laksbang Mediatama, 2009.

Qardhawi, Yusuf, Muhamad Madani dan Mu'imuddin Qadri. *Dasar Pemikiran Hukum Islam; Taqlid Versus Ijtihad*. Cet. III; Jakarta: Pustaka Firdaus, 2003.

Zahrah, Muhammad Abu. *Al-Jarimah wa al-'Uqubah fi al-Fikr al-Islamiy*. [t.t.]: Dar al-Fikr al-'Arabi, [t.th].

Zuhaili, Wahbah. *Al-Fiqh al-Islami wa Adillatuhu*. Damaskus: Dar al-Fikr, 1989.

DAFTAR RIWAYAT HIDUP



Nama : **MOHAMMAD HAIDAR ALI**

Tempat/

tanggal lahir : Banyuwangi, 02 Mei 1982

Pekerjaan : Wiraswasta

Alamat : Danau Mahalona No. 31 Taman Toraja Rt/Rw: 002/007
Tanjung Merdeka Tamalate Makassar Sulawesi Selatan

Nama Ayah : H. Alit Sukardi AM

Nama Ibu : Almarhumah Hj. Musri'ah

Alamat Orang Tua : Dusun Krajan I Desa Tegalsari Kecamatan Tegalsari
Kabupaten Banyuwangi Provinsi Jawa Timur

Urutan dalam Keluarga : Anak ke sembilan dari sepuluh bersaudara

Riwayat Pendidikan :

1. Madrasah Ibtidaiyah (MI) Tegalsari II, tamat tahun 1995;
2. Madrasah Tsanawiyah (MTs) Diponegoro Tegalsari, tamat tahun 1998;
3. Sekolah Menengah Umum (SMU) Nurul Jadid Paiton Probolinggo, tamat tahun 2001;
4. S.1 Fakultas Syariah Ahwalul Syakhshiyah STAIN Ambon, tamat tahun 2006;
5. S.2 Konsentrasi Syariah/Hukum Islam pada Program Pascasarjana UIN Alauddin Makassar 2008 s/d sekarang.

Pengalaman Organisasi :

1. Ketua Himpunan Mahasiswa Jurusan (HMJ) Syariah STAIN Ambon periode 2004-2005;
2. Ketua Bidang Finansial dan Sosial Masyarakat KSR-PMI unit STAIN Ambon periode 2004-2005 dan 2005-2006;

3. Sekretaris Umum Kesatuan Aksi Mahasiswa Muslim Indonesia (KAMMI) Komisariat STAIN Ambon periode 2004-2005;
4. Staf Kaderisasi Lembaga Dakwah Kampus (LDK) Al-'Izzah STAIN Ambon periode 2004-2005.

Karya Tulis :

1. Nikah Mut'ah Menurut Tinjauan Hukum Islam (skripsi)
2. *Cyber Crime* Menurut Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Perspektif Hukum Pidana Islam (tesis).

Pengalaman Mengajar :

1. Guru Madrasah Tsanawiyah (MTs) Nurul Huda Seram Utara Maluku Tengah tahun 2007-2008;
2. Guru Madrasah Aliyah (MA) Nurul Huda Seram Utara Maluku Tengah tahun 2007-2008.

Selama menempuh jenjang pendidikan tingkat SLTA, saya juga pernah menetap di salah satu Pondok Pesantren (Ponpes) di Paiton Probolinggo tahun 1998-2001 di bawah asuhan Drs. KH. Abdul Wahid Zaini, SH.

Selama di pesantren saya juga aktif di organisasi kepesantrenan seperti Aliansi Murid Diniyah (ALMURADI) dan Ikatan Santri Banyuwangi (IKAWANGI).

Demikian daftar riwayat hidup ini saya buat dengan sebenarnya dan apabila ada ketidakbenaran dapat dituntut sesuai dengan hukum.

Makassar, Oktober 2012

Mohammad Haidar Ali

LAMPIRAN 1

JENIS DAN SANKSI PIDANA *CYBER CRIME* DALAM UU ITE

No.	Jenis Pidana	Pasal	Ayat	Subyek	Obyek	Sanksi Pidana
				Pidana		
1.	Pornografi	27	(1)	-	-	6 Thn dan denda Rp. 1 miliar
		45	(1)	-	-	
		52	(1)	-	Anak	Sepertiga dari pidana pokok Pidana pokok ditambah dua pertiga
			(4)	Korporasi	-	
2.	Perjudian	27	(2)	-	-	6 Thn dan denda Rp. 1 miliar
		45	(1)	-	-	
		52	(4)	Korporasi	-	Pidana pokok ditambah dua pertiga
3.	Penghinaan/Pencemaran Nama Baik	27	(3)	-	-	6 Thn dan denda Rp. 1 miliar
		45	(1)	-	-	
		52	(4)	Korporasi	-	Pidana pokok ditambah dua pertiga
4.	Pemerasan/Pengancaman	27	(4)	-	-	6 Thn dan denda Rp. 1 miliar
		45	(1)	-	-	
		52	(4)	Korporasi	-	Pidana pokok ditambah dua pertiga
5.	Penipuan	28	(1)	-	-	6 Thn dan denda Rp. 1 miliar
		45	(2)	-	-	
6.	Menyebarkan Kebencian, Penghasutan	28	(2)	-	-	6 Thn dan denda Rp. 1 miliar
		45	(2)	-	-	
7.	Pengancaman	29	-	-	-	12 Thn dan denda Rp. 2 miliar
		45	(3)	-	-	
8.	Pencurian/Penggelapan/ Penerobosan/Akses Tanpa Izin Hak	30/46	(1)/(1)	-	-	6 Thn dan denda Rp. 600 juta
			(2)/(2)	-	-	7 Thn dan denda Rp. 700 juta
			(3)/(3)	-	-	8 Thn dan denda Rp. 800 juta
		52	(2)	-	Milik Pemerintah Untuk Publik	Pidana pokok ditambah sepertiga
			(3)	-	Milik Pemerintah/ Badan setrategis	Pidana pokok ditambah dua pertiga
9.	Penyadapan	31/47	(1)/(1)	-	-	10 Thn dan denda Rp. 800 juta
			(2)/(2)	-	-	
			(3)	-	-	
			(4)	-	-	
		52	(2)	-	Milik Pemerintah	Pidana pokok ditambah sepertiga

					Untuk Publik	
			(3)	-	Milik Pemerintah/ Badan setrategis	Pidana pokok ditambah dua pertiga
10.	Pemalsuan Data/ Pembocoran Rahasia	32/48	(1)/(1)	-	-	8 Thn dan denda Rp. 2 miliar
			(2)/(2)	-	-	9 Thn dan denda Rp. 3 miliar
			(3)/(3)	-	-	10 Thn dan denda Rp. 5 miliar
		52	(2)	-	Milik Pemerintah Untuk Publik	Pidana pokok ditambah sepertiga
			(3)	-	Milik Pemerintah/ Badan setrategis	Pidana pokok ditambah dua pertiga
11.	Sabotase dan Perusakan	33/49	-	-	-	10 Thn dan denda Rp. 10 miliar
		52	(2)	-	Milik Pemerintah Untuk Publik	Pidana pokok ditambah sepertiga
			(3)	-	Milik Pemerintah/ Badan setrategis	Pidana pokok ditambah dua pertiga
12.	Tanpa Izin/Pembajakan (Perbuatan Pidana) HAKI	34	(1)	-	-	10 Thn dan denda Rp. 10 miliar
		50	-	-	-	
		52	(2)	-	Milik Pemerintah Untuk Publik	Pidana pokok ditambah sepertiga
			(3)	-	Milik Pemerintah/ Badan setrategis	Pidana pokok ditambah dua pertiga
13.	Pemalsuan	35	-	-	-	12 Thn dan denda Rp. 10 miliar
		51	(1)	-	-	
		52	(2)	-	Milik Pemerintah Untuk Publik	Pidana pokok ditambah sepertiga
			(3)	-	Milik Pemerintah/ Badan setrategis	Pidana pokok ditambah dua pertiga

14.	Kejahatan Kartu Kredit	28/45	(1)/(2)	-	-	6 Thn dan denda Rp. 1 miliar
		30/46	(1)/(1)	-	-	6 Thn dan denda Rp. 600 juta
			(2)/(2)	-	-	7 Thn dan denda Rp. 700 juta
			(3)/(3)	-	-	8 Thn dan denda Rp. 800 juta
		32/48	(1)/(1)	-	-	8 Thn dan denda Rp. 2 miliar
			(2)/(2)	-	-	9 Thn dan denda Rp. 3 miliar
			(3)/(3)	-	-	10 Thn dan denda Rp. 5 miliar
		33/49	-	-	-	10 Thn dan denda Rp. 10 miliar
		35/51	-(1)	-	-	12 Thn dan denda Rp. 10 miliar
		36/51	-(2)	-	-	12 Thn dan denda Rp. 12 miliar
		37/52	-(2)	-	-	Pidana pokok ditambah sepertiga
			-(3)	-	-	Pidana pokok ditambah dua pertiga
			-(4)	-	-	Pidana pokok ditambah dua pertiga

LAMPIRAN 2

UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008

TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

**DENGAN RAHMAT TUHAN YANG MAHA ESA
PRESIDEN REPUBLIK INDONESIA,**

Menimbang:

- a. bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat;
- b. bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa;
- c. bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru;
- d. bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkuat persatuan dan kesatuan nasional berdasarkan Peraturan Perundang-undangan demi kepentingan nasional;
- e. bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat;
- f. bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia;

- g. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f, perlu membentuk Undang-Undang tentang Informasi dan Transaksi Elektronik;

Mengingat:

Pasal 5 ayat (1) dan Pasal 20 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

Dengan Persetujuan Bersama
DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA
 dan
PRESIDEN REPUBLIK INDONESIA

MEMUTUSKAN:

Menetapkan:

**UNDANG-UNDANG
 TENTANG
 INFORMASI DAN TRANSAKSI ELEKTRONIK**

**BAB I
 KETENTUAN UMUM**

Pasal 1

Dalam Undang-Undang ini yang dimaksud dengan:

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), Surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.
3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memroses, mengumumkan, menganalisis, dan/atau menyebarkan Informasi.
4. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital,

elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
6. Penyelenggaraan Sistem Elektronik adalah pemanfaatan sistem elektronik oleh penyelenggara negara, orang, badan usaha, dan/atau masyarakat.
7. Jaringan Sistem Elektronik adalah terhubungnya dua sistem elektronik atau lebih, yang bersifat tertutup atau pun terbuka.
8. Agen Elektronik adalah perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh orang.
9. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
10. Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik.
11. Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.
12. Tanda Tangan Elektronik adalah tandatangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
13. Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan tanda tangan elektronik.
14. Komputer adalah alat untuk memroses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.
15. Akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan.

16. Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses komputer dan/atau sistem elektronik lainnya.
17. Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui sistem elektronik.
18. Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau dokumen elektronik.
19. Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau dokumen elektronik dari pengirim.
20. Nama Domain adalah alamat internet penyelenggara negara, orang, badan usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
22. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
23. Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

Pasal 2

Undang-Undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

BAB II **ASAS DAN TUJUAN**

Pasal 3

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Pasal 4

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

- a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat Informasi dunia;
- b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
- c. meningkatkan efektivitas dan efisiensi pelayanan publik;
- d. membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan
- e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

BAB III INFORMASI, DOKUMEN, DAN TANDA TANGAN ELEKTRONIK

Pasal 5

- (1) Informasi Elektronik dan/atau Dokumen Elektronik dan/ atau hasil cetaknya merupakan alat bukti hukum yang sah.
- (2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
- (3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.
- (4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
 - a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
 - b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.

Pasal 6

Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang menyatakan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang

tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Pasal 7

Setiap orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan.

Pasal 8

- (1) Kecuali diperjanjikan lain, waktu pengiriman suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik telah dikirim dengan alamat yang benar oleh Pengirim ke suatu Sistem Elektronik yang ditunjuk atau dipergunakan Penerima dan telah memasuki Sistem Elektronik yang berada di luar kendali Pengirim.
- (2) Kecuali diperjanjikan lain, waktu penerimaan suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik di bawah kendali Penerima yang berhak.
- (3) Dalam hal Penerima telah menunjuk suatu Sistem Elektronik tertentu untuk menerima Informasi Elektronik, penerimaan terjadi pada saat Informasi Elektronik dan/ atau Dokumen Elektronik memasuki Sistem Elektronik yang ditunjuk.
- (4) Dalam hal terdapat dua atau lebih Sistem Informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau Dokumen Elektronik, maka:
 - a. waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim;
 - b. waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi terakhir yang berada di bawah kendali Penerima.

Pasal 9

Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

Pasal 10

- (1) Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.
- (2) Ketentuan mengenai pembentukan Lembaga Sertifikasi Keandalan sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 11

- (1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:
 - a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
 - b. data pembuatan Tanda Tangan Elektronik pada saat proses penanda tangan elektronik hanya berada dalam kuasa Penanda Tangan;
 - c. segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
 - d. segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
 - e. terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatanggannya; dan
 - f. terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.
- (2) Ketentuan lebih lanjut tentang Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 12

- (1) Setiap Orang yang terlibat dalam Tanda Tangan Elektronik berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya.
- (2) Pengamanan Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) sekurang-kurangnya meliputi:
 - a. sistem tidak dapat diakses oleh orang lain yang tidak berhak;
 - b. Penanda Tangan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;
 - c. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik atau pun cara lain

yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:

Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; atau keadaan yang diketahui oleh penanda tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan

- d. dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.
- (3) Setiap orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud pada ayat (1), bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.

BAB IV

PENYELENGGARAAN SERTIFIKASI ELEKTRONIK DAN SISTEM ELEKTRONIK

BAGIAN KESATU

PENYELENGGARAAN SERTIFIKASI ELEKTRONIK

Pasal 13

- (1) Setiap orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.
- (2) Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.
- (3) Penyelenggara Sertifikasi Elektronik terdiri atas:
 - a. Penyelenggara Sertifikasi Elektronik Indonesia; dan
 - b. Penyelenggara Sertifikasi Elektronik asing.
- (4) Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.
- (5) Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.
- (6) Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 14

Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud dalam Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi:

- a. metode yang digunakan untuk mengidentifikasi Penanda Tangan;
- b. hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik; dan
- c. hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

BAGIAN KEDUA PENYELENGGARAAN SISTEM ELEKTRONIK

Pasal 15

- (1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
- (2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
- (3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 16

- (1) Sepanjang tidak ditentukan lain oleh Undang-Undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:
 - a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
 - b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
 - c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;

- d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
 - e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan keberanggungan prosedur atau petunjuk.
- (2) Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

BAB V TRANSAKSI ELEKTRONIK

Pasal 17

- (1) Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik atau pun privat.
- (2) Para pihak yang melakukan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) wajib beritikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung.
- (3) Ketentuan lebih lanjut mengenai penyelenggaraan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 18

- (1) Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak.
- (2) Para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya.
- (3) Jika para pihak tidak melakukan pilihan hukum dalam Transaksi Elektronik internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata International.
- (4) Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari Transaksi Elektronik internasional yang dibuatnya.
- (5) Jika para pihak tidak melakukan pilihan forum sebagaimana dimaksud pada ayat (4), penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata International.

Pasal 19

Para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang disepakati.

Pasal 20

- (1) Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.
- (2) Persetujuan atas penawaran Transaksi Elektronik sebagaimana dimaksud pada ayat (1) harus dilakukan dengan pernyataan penerimaan secara elektronik.

Pasal 21

- (1) Pengirim atau Penerima dapat melakukan Transaksi Elektronik sendiri, melalui pihak yang dikuasakan olehnya, atau melalui agen elektronik.
- (2) Pihak yang bertanggungjawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:
 - a. jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi;
 - b. jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggungjawab pemberi kuasa; atau
 - c. jika dilakukan melalui agen elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara agen elektronik.
- (3) Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya agen elektronik akibat tindakan pihak ketiga secara langsung terhadap sistem elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara agen elektronik.
- (4) Jika kerugian transaksi elektronik disebabkan gagal beroperasinya agen elektronik akibat kelalaian pihak pengguna jasa layanan, segala akibat hukum menjadi tanggung jawab pengguna jasa layanan.
- (5) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 22

- (1) Penyelenggara Agen Elektronik tertentu harus menyediakan fitur pada agen elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi.
- (2) Ketentuan lebih lanjut mengenai penyelenggara Agen Elektronik tertentu sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

BAB VI

**NAMA DOMAIN, HAK KEKAYAAN INTELEKTUAL,
DAN PERLINDUNGAN HAK PRIBADI**

Pasal 23

- (1) Setiap penyelenggara negara, orang, badan usaha, dan/atau masyarakat berhak memiliki nama domain berdasarkan prinsip pendaftar pertama.
- (2) Pemilikan dan penggunaan nama domain sebagaimana dimaksud pada ayat (1) harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak orang lain.
- (3) Setiap penyelenggara negara, orang, badan usaha, atau masyarakat yang dirugikan karena penggunaan nama domain secara tanpa hak oleh orang lain, berhak mengajukan gugatan pembatalan nama domain dimaksud.

Pasal 24

- (1) Pengelola nama domain adalah pemerintah dan/atau masyarakat.
- (2) Dalam hal terjadi perselisihan pengelolaan nama domain oleh masyarakat, pemerintah berhak mengambil alih sementara pengelolaan nama domain yang diperselisihkan.
- (3) Pengelola nama domain yang berada di luar wilayah Indonesia dan nama domain yang diregistrasinya diakui keberadaannya sepanjang tidak bertentangan dengan Peraturan Perundang-undangan.
- (4) Ketentuan lebih lanjut mengenai pengelolaan nama domain sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 25

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Pasal 26

- (1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.
- (2) Setiap orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

BAB VII PERBUATAN YANG DILARANG

Pasal 27

- (1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
- (2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
- (3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
- (4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 28

- (1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
- (2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Pasal 29

Setiap orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
- (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
- (3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian,

kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan Undang-Undang.

- (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak.
- (3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
 - a. perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
 - b. Sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
- (2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 36

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain.

Pasal 37

Setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

BAB VIII PENYELESAIAN SENGKETA

Pasal 38

- (1) Setiap orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang menimbulkan kerugian.
- (2) Masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan sistem elektronik dan/atau menggunakan Teknologi Informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan Peraturan Perundang-undangan.

Pasal 39

- (1) Gugatan perdata dilakukan sesuai dengan ketentuan Peraturan Perundang-undangan.
- (2) Selain penyelesaian gugatan perdata sebagaimana dimaksud pada ayat (1), para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan.

BAB IX

PERAN PEMERINTAH DAN PERAN MASYARAKAT

Pasal 40

- (1) Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan Peraturan Perundang-undangan.
- (2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan.
- (3) Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi.
- (4) Instansi atau institusi sebagaimana dimaksud pada ayat harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data.
- (5) Instansi atau institusi lain selain diatur pada ayat (3) membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya.
- (6) Ketentuan lebih lanjut mengenai peran pemerintah sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat diatur dengan Peraturan Pemerintah.

Pasal 41

- (1) Masyarakat dapat berperan meningkatkan pemanfaatan Teknologi Informasi melalui penggunaan dan Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik sesuai dengan ketentuan Undang-Undang ini.
- (2) Peran masyarakat sebagaimana dimaksud pada ayat (1) dapat diselenggarakan melalui lembaga yang dibentuk oleh masyarakat.
- (3) Lembaga sebagaimana dimaksud pada ayat (2) dapat memiliki fungsi konsultasi dan mediasi.

BAB X

PENYIDIKAN

Pasal 42

Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini.

Pasal 43

- (1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.
- (2) Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.
- (3) Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat.
- (4) Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.
- (5) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:
 - a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana berdasarkan ketentuan Undang-Undang ini;
 - b. memanggil setiap orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang terkait dengan ketentuan Undang-Undang ini;
 - c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana berdasarkan ketentuan Undang-Undang ini;
 - d. melakukan pemeriksaan terhadap orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana berdasarkan Undang-Undang ini;
 - e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-Undang ini;
 - f. melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana berdasarkan ketentuan Undang-Undang ini;

- g. melakukan penyegelan dan penyitaan terhadap alat dan atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan Peraturan Perundang-undangan;
 - h. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini; dan/atau
 - i. mengadakan penghentian penyidikan tindak pidana berdasarkan Undang-Undang ini sesuai dengan ketentuan hukum acara pidana yang berlaku.
- (6) Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.
- (7) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Penyidik Pejabat Polisi Negara Republik Indonesia memberitahukan dimulainya penyidikan dan menyampaikan hasilnya kepada penuntut umum.
- (8) Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.

Pasal 44

Alas bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

- a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
- b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

BAB XI KETENTUAN PIDANA

Pasal 45

- (1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

- (2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).
- (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah).

Pasal 46

- (1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).
- (2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).
- (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Pasal 47

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Pasal 48

- (1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah).
- (2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp 3.000.000.000,00 (tiga miliar rupiah).
- (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah).

Pasal 49

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah).

Pasal 50

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah).

Pasal 51

- (1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).
- (2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).

Pasal 52

- (1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.
- (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap komputer dan/atau sistem elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik pemerintah dan/ atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.
- (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap komputer dan/atau sistem elektronik serta Informasi Elektronik dan/ atau Dokumen Elektronik milik pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank central, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.
- (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

BAB XII **KETENTUAN PERALIHAN**

Pasal 53

Pada saat berlakunya Undang-Undang ini, semua Peraturan Perundang-undangan dan kelembagaan yang berhubungan dengan pemanfaatan Teknologi Informasi yang tidak bertentangan dengan Undang-Undang ini dinyatakan tetap berlaku.

BAB XIII

KETENTUAN PENUTUP

Pasal 54

- (1) Undang-Undang ini mulai berlaku pada tanggal diundangkan.
- (2) Peraturan Pemerintah harus sudah ditetapkan paling lama 2 (dua) tahun setelah diundangkannya Undang-Undang ini.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Undang-Undang ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Disahkan di Jakarta
pada tanggal 21 April 2008

**MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA**

ANDI MATTALATA

**LEMBARAN NEGARA REPUBLIK INDONESIA
TAHUN 2008 NOMOR 58**

LAMPIRAN 3

PENJELASAN ATAS UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

I. UMUM

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*border-less*) dan menyebabkan perubahan social, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyberlaw*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang

dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Yang dimaksud dengan sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk

mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memroses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input, process, output, storage, dan communication*.

Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelian di Internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit.

Permasalahan yang lebih luas terjadi pada bidang keperdataan karena transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik (*electronic commerce*) telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru di bidang teknologi informasi, media, dan komunikasi.

Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (*cyber space*), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan

hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alas buktinya bersifat elektronik.

Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai Orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* antara lain dikenal adanya dokumen elektronik yang kedudukannya disetarakan dengan dokumen yang dibuat di atas kertas.

Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan di *cyber space*, yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

II. PASAL DEMI PASAL

Pasal 1

Cukup jelas.

Pasal 2

Undang-Undang ini memilikijangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal.

Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

Pasal 3

"Asas kepastian hukum" berarti landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.

"Asas manfaat" berarti asas bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat.

"Asas kehati-hatian" berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun bagi pihak lain dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik.

"Asas iktikad baik" berarti asas yang digunakan para pihak dalam melakukan Transaksi Elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut.

"Asas kebebasan memilih teknologi atau netral teknologi" berarti asas pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

Pasal 4

Cukup jelas.

Pasal 5

Ayat 1
Cukup jelas.

Ayat 2
Cukup jelas.

Ayat 3
Cukup jelas

Ayat 4
Huruf a

Surat yang menurut undang-undang harus dibuat tertulis meliputi tetapi tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara.

Huruf b
Cukup jelas.

Pasal 6

Selama ini bentuk tertulis identik dengan informasi dan/ atau dokumen yang tertuang di atas kertas semata, padahal pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik. Dalam lingkup Sistem Elektronik, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab Sistem Elektronik pada dasarnya beroperasi dengan cara penggandaan yang mengakibatkan informasi yang asli tidak dapat dibedakan lagi dari salinannya.

Pasal 7

Ketentuan ini dimaksudkan bahwa suatu Informasi Elektronik dan/atau Dokumen Elektronik dapat digunakan sebagai alasan timbulnya suatu hak.

Pasal 8

Cukup jelas.

Pasal 9

Yang dimaksud dengan "informasi yang lengkap dan benar" meliputi:

- a. informasi yang memuat identitas serta status subjek hukum dan kompetensinya, baik sebagai produsen, pemasok, penyelenggara maupun perantara;
- b. informasi lain yang menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan/atau jasa yang ditawarkan, seperti nama, alamat, dan deskripsi barang/jasa.

Pasal 10

Ayat (1)

Sertifikasi Keandalan dimaksudkan sebagai bukti bahwa pelaku usaha yang melakukan perdagangan secara elektronik layak berusaha setelah melalui penilaian dan audit dari badan yang berwenang. Bukti telah dilakukan Sertifikasi Keandalan ditunjukkan dengan adanya logo sertifikasi berupa *trust mark* pada halaman (*home page*) pelaku usaha tersebut.

Ayat (2)

Cukup jelas.

Pasal 11

Ayat (1)

Undang-Undang ini memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, Tanda Tangan Elektronik memiliki kedudukan yang sama

dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum.

Persyaratan sebagaimana dimaksud dalam Pasal ini merupakan persyaratan minimum yang harus dipenuhi dalam setiap Tanda Tangan Elektronik. Ketentuan ini membuka kesempatan seluas-luasnya kepada siapa pun untuk mengembangkan metode, teknik, atau proses pembuatan Tanda Tangan Elektronik.

Ayat (2)

Peraturan Pemerintah dimaksud, antara lain, mengatur tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik.

Pasal 12

Cukup jelas.

Pasal 13

Cukup jelas.

Pasal 14

Informasi sebagaimana dimaksud dalam Pasal ini adalah informasi yang minimum harus dipenuhi oleh setiap penyelenggara Tanda Tangan Elektronik.

Pasal 15

Ayat (1)

"Andal" artinya Sistem Elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya. "Aman" artinya Sistem Elektronik terlindungi secara fisik dan nonfisik.

"Beroperasi sebagaimana mestinya" artinya Sistem Elektronik memiliki kemampuan sesuai dengan spesifikasinya.

Ayat (2)

"Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap Penyelenggaraan Sistem Elektronik tersebut.

Ayat (3)

Cukup jelas.

Pasal 16

Cukup jelas.

Pasal 17

Ayat (1)

Undang-Undang ini memberikan peluang terhadap pemanfaatan Teknologi Informasi oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.

Pemanfaatan Teknologi Informasi harus dilakukan secara baik, bijaksana, bertanggung jawab, efektif, dan efisien agar dapat diperoleh manfaat yang sebesar-besarnya bagi masyarakat.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 18

Ayat (1)

Cukup jelas.

Ayat (2)

Pilihan hukum yang dilakukan oleh para pihak dalam kontrak internasional termasuk yang dilakukan secara elektronik dikenal dengan *choice of law*. Hukum ini mengikat sebagai hukum yang berlaku bagi kontrak tersebut.

Pilihan hukum dalam Transaksi Elektronik hanya dapat dilakukan jika dalam kontraknya terdapat unsur asing dan penerapannya harus sejalan dengan prinsip Hukum Perdata Internasional (HPI).

Ayat (3)

Dalam hal tidak ada pilihan hukum, penetapan hukum yang berlaku berdasarkan prinsip atau asas hukum perdata internasional yang akan ditetapkan sebagai hukum yang berlaku pada kontrak tersebut.

Ayat (4)

Forum yang berwenang mengadili sengketa kontrak internasional, termasuk yang dilakukan secara elektronik, adalah forum yang dipilih oleh para pihak. Forum tersebut dapat berbentuk pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya.

Ayat (5)

Dalam hal para pihak tidak melakukan pilihan forum, kewenangan forum berlaku berdasarkan prinsip atau asas hukum perdata internasional. Asas tersebut dikenal

dengan asas tempat tinggal tergugat (*the basis of presence*) dan efektivitas yang menekankan pada tempat harta benda tergugat berada (*principle of effectiveness*).

Pasal 19

Yang dimaksud dengan "disepakati" dalam pasal ini juga mencakup disepakatinya prosedur yang terdapat dalam Sistem Elektronik yang bersangkutan.

Pasal 20

Ayat (1)

Transaksi Elektronik terjadi pada saat kesepakatan antara para pihak yang dapat berupa, antara lain pengecekan data, identitas, nomor identifikasi pribadi (*personal identification number/PIN*) atau Sandi lewat (*password*).

Ayat (2)

Cukup jelas.

Pasal 21

Ayat (1)

Yang dimaksud dengan "dikuasakan" dalam ketentuan ini sebaiknya dinyatakan dalam Surat kuasa.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Pasal 22

Ayat (1)

Yang dimaksud dengan "fitur" adalah fasilitas yang memberikan kesempatan kepada pengguna Agen Elektronik untuk melakukan perubahan atas informasi yang disampaikan, misalnya fasilitas pembatalan (*cancel*), edit, dan konfirmasi ulang.

Ayat (2)

Cukup jelas.

Pasal 23

Ayat (1)

Nama Domain berupa alamat atau jati diri penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang perolehannya didasarkan pada prinsip pendaftar pertama (*first come first serve*).

Prinsip pendaftar pertama berbeda antara ketentuan dalam Nama Domain dan dalam bidang hak kekayaan intelektual karena tidak diperlukan pemeriksaan substantif, seperti pemeriksaan dalam pendaftaran merek dan paten.

Ayat (2)

Yang dimaksud dengan "melanggar hak Orang lain", misalnya melanggar merek terdaftar, nama badan hukum terdaftar, nama Orang terkenal, dan nama sejenisnya yang pada intinya merugikan Orang lain.

Ayat (3)

Yang dimaksud dengan "penggunaan Nama Domain secara tanpa hak" adalah pendaftaran dan penggunaan Nama Domain yang semata-mata ditujukan untuk menghalangi atau menghambat Orang lain untuk menggunakan nama yang intuitif dengan keberadaan nama dirinya atau nama produknya, atau untuk mendompleng reputasi Orang yang sudah terkenal atau ternama, atau untuk menyesatkan konsumen.

Pasal 24

Cukup jelas.

Pasal 25

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun dan didaftarkan sebagai karya intelektual, hak cipta, paten, merek, rahasia dagang, desain industri, dan sejenisnya wajib dilindungi oleh Undang-Undang ini dengan memperhatikan ketentuan Peraturan Perundang-undangan.

Pasal 26

Ayat (1)

Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut:

- a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.

- b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
- c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Ayat (2)

Cukup jelas.

Pasal 27

Cukup jelas.

Pasal 28

Cukup jelas.

Pasal 29

Cukup jelas.

Pasal 30

Ayat (1)

Cukup jelas.

Ayat (2)

Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:

- a. melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau
- b. sengaja menghalangi agar informasi dimaksud tidak dapat atau gaga) diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

Ayat (3)

Sistem pengamanan adalah sistem yang membatasi akses Komputer atau melarang akses ke dalam Komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan.

Ayat (2)

Cukup jelas.

Ayat (3)
Cukup jelas.

Ayat (4)
Cukup jelas.

Pasal 32
Cukup jelas.

Cukup jelas. Pasal 33

Pasal 34
Ayat (1)
Cukup jelas.

Ayat (2)
Yang dimaksud dengan "kegiatan penelitian" adalah penelitian yang dilaksanakan oleh lembaga penelitian yang memiliki izin.

Pasal 35
Cukup jelas.

Pasal 36
Cukup jelas.

Pasal 37
Cukup jelas.

Pasal 38
Cukup jelas.

Pasal 39
Cukup jelas.

Pasal 40
Cukup jelas

Pasal 41

Ayat (1)
Cukup jelas.

Ayat (2)

Yang dimaksud dengan "lembaga yang dibentuk oleh masyarakat" merupakan lembaga yang bergerak di bidang teknologi informasi dan transaksi elektronik.

Ayat (3)

Cukup jelas.

Pasal 42

Cukup jelas.

Pasal 43

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

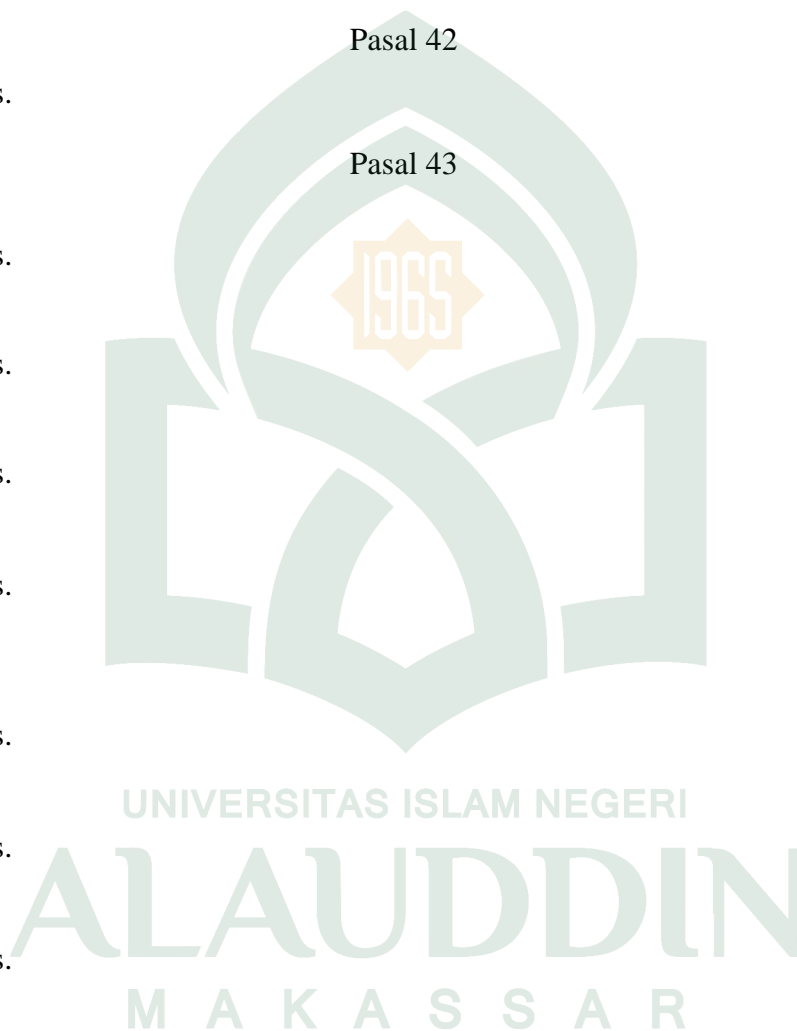
Cukup jelas.

Huruf e

Cukup jelas.

Huruf f

Cukup jelas.



Huruf g
Cukup jelas.

Huruf h
Yang dimaksud dengan "ahli" adalah seseorang yang memiliki keahlian khusus di bidang Teknologi Informasi yang dapat dipertanggungjawabkan secara akademis maupun praktis mengenai pengetahuannya tersebut.

Huruf i
Cukup jelas.

Ayat (6)
Cukup jelas.

Ayat (7)
Cukup jelas.

Ayat (8)
Cukup jelas.

Cukup jelas.

Cukup jelas.

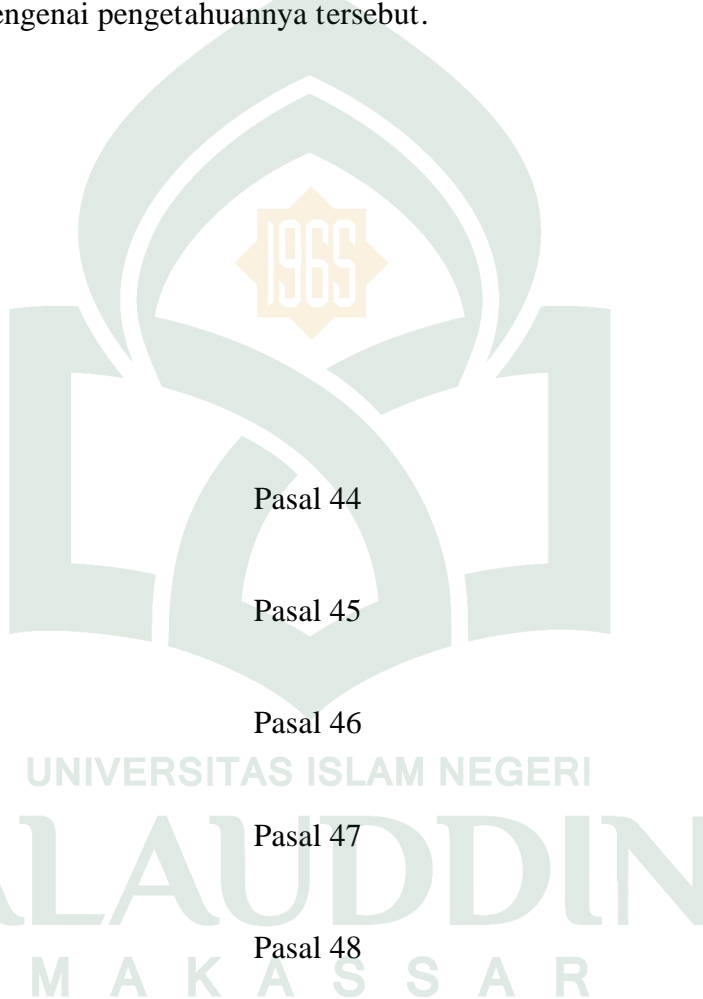
Cukup jelas.

Cukup jelas.

Cukup jelas.

Cukup jelas.

Cukup jelas.



Pasal 51

Cukup jelas.

Pasal 52

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Ketentuan ini dimaksudkan untuk menghukum setiap perbuatan melawan hukum yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 yang dilakukan oleh korporasi (*corporate crime*) dan/atau oleh pengurus dan/atau staf yang memiliki kapasitas untuk:

- a. mewakili korporasi;
- b. mengambil keputusan dalam korporasi;
- c. melakukan pengawasan dan pengendalian dalam korporasi;
- d. melakukan kegiatan demi keuntungan korporasi.

Pasal 53

Cukup jelas.

Pasal 54

Cukup jelas.

TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA
NOMOR 4843



Tesis ini membahas tentang *cyber crime* menurut Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik perspektif hukum pidana Islam. Adapun masalah yang dikemukakan dalam tesis ini adalah sebagai berikut; *Pertama*, bagaimana hakikat *cyber crime* dan eksistensinya dalam Undang-Undang ITE? *Kedua*, bagaimana perspektif hukum pidana Islam tentang *cyber crime*? *Ketiga*, bagaimana bentuk sanksi pidana *cyber crime* menurut hukum pidana di Indonesia dan hukum pidana Islam? Adapun tujuan dari penelitian ini adalah untuk mengetahui hakikat *cyber crime* dan eksistensinya dalam Undang-Undang ITE, untuk mengetahui *cyber crime* menurut perspektif hukum pidana Islam, dan untuk mengetahui bentuk sanksi pidana *cyber crime* menurut hukum pidana di Indonesia dan hukum pidana Islam.

Untuk mengurai lebih jauh pokok permasalahan dalam tesis ini, mengacu pada pendekatan *multidisipliner* yaitu pendekatan teologis normatif (*syar'i*), yuridis normatif, sosiologis dan historis. Penelitian ini tergolong *library research* yang dikumpulkan dari buku-buku dan literatur yang berhubungan dengan pembahasan. Selanjutnya data yang diperoleh diinventarisir diseleksi sesuai dengan masalah tersebut dan dikaji serta dianalisis dengan metode kualitatif eksplanatif dan dengan *content analysis* (analisis isi).

Hasil dari penelitian ini mengungkapkan beberapa hal yaitu; *pertama*, *cyber crime* dalam Undang-Undang ITE pada hakikatnya adalah kejahatan yang dilakukan oleh pelaku dengan menggunakan sarana teknologi informasi (internet) dan sejenisnya. Perbuatan *cyber crime* telah diatur secara spesifik melalui Undang-Undang ITE tercantum dalam Bab 7 untuk "Perbuatan yang Dilarang" yakni pada Pasal 27-37 dan dalam Bab 11 untuk "Ketentuan Pidana" pada Pasal 45-52. *Kedua*, hukum pidana Islam melihat *cyber crime* sebagai suatu kejahatan nyata, tetapi maya yang mengalami modernisasi pada aspek modus operandi dan memiliki kesamaan terhadap hukum pidana Islam pada aspek substansi. Karena kejahatan yang terjadi pada dunia *cyber* merupakan pengembangan dari bentuk kejahatan yang cikal bakalnya telah ada pada zaman dahulu kala dan berkembang secara pesat melalui perkembangan teknologi informasi. Kejahatan yang terlihat pada saat ini merupakan bentuk modernisasi yang mengiringi perkembangan *cyber space* (dunia maya/internet). *Cyber crime* dilihat dari sudut pandang hukum pidana Islam yang menjadi landasan pokok terhadap aspek yuridis, adalah teori *maqasid al-syar'iah* meletakkan prinsip-prinsip yang menjadi pertimbangan pokok dari tujuan hukum, yaitu terwujudnya kemaslahatan manusia baik di dunia maupun di akhirat, yaitu terwujud dan terpeliharanya *al-masāliḥ al-khamsah* atau lima kebutuhan pokok dalam kehidupan manusia yang mencakup pemeliharaan agama (*hiḥẓ al-dīn*), jiwa (*hiḥẓ al-nafs*), keturunan atau kehormatan (*hiḥẓ al-nasl*), harta (*hiḥẓ al-māl*) dan akal (*hiḥẓ al-'aql*). Sehingga kenyataan dalam praktik-praktik *cyber crime* dinilai melanggar lima kebutuhan pokok dalam kehidupan manusia tersebut. *Ketiga*, adapun sanksi pidana bagi penipuan, kesusilaan, perjudian, pengancaman, pengrusakan, dan pencurian dapat dilihat dalam Undang-Undang ITE. Sedangkan dalam hukum pidana Islam, sanksi pidana ditentukan berdasarkan *jarimah ḥudud*, *jarimah qisās* dan diat, dan *jarimah ta'zīr*.

Rekomendasi dari penelitian ini adalah, bahwa reregulasi dan optimalisasi esensi hukum dan perundang-undangan di Indonesia diperlukan untuk mewujudkan *law an forcemnt* dan kepastian hukum. Hal ini didasarkan oleh lahirnya banyak perundang-undangan yang kurang menyentuh substansi hukum, yakni terciptanya rasa keadilan, keamanan dan ketentraman masyarakat.